A Bibliography of Publications on Cryptography: 2000–2009

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148

E-mail: `beebe@math.utah.edu`, `beebe@acm.org`, `beebe@computer.org` (Internet)
WWW URL: `https://www.math.utah.edu/~beebe/`

03 June 2024
Version 3.341

Title word cross-reference

References

XXX:2002:CC

[??02] ?? *Codes Ciphers*. Bounty Books, 2002. ISBN 0-7537-0220-7. LCCN ???? UK£7.99.

Al-Akaidi:2004:FSP

[AA04a] Marwan Al-Akaidi. *Fractal speech processing*. Cambridge University Press, Cambridge, UK, 2004. ISBN 0-521-81458-8 (hardcover), 0-511-75454-X (e-book). x + 214 pp. LCCN TK7882.S65 A43 2004; TK7882.S65 ALA. URL http://www.loc.gov/catdir/description/cam032/2003055750.htm; http://www.loc.gov/catdir/toc/cam032/2003055750.htm.

Aly:2004:CSP

[AA04b] Alaaeldin A. Aly and Shakil Akhtar. Cryptography and security protocols course for undergraduate IT students. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 36(2):44–47, June 2004. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). URL https://www.math.utah.edu/pub/mirrors/ftp.ira.uka.de/bibliography/Misc/DBLP/2004.bib.

Agreste:2008:NAP

[AA08] Santa Agreste and Guido

Andaloro. A new approach to pre-processing digital image for wavelet-based watermark. *Journal of Computational and Applied Mathematics*, 221(2):274–283, November 15, 2008. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042707005602.

Apers:2001:PTS

[AAC+01] Peter M. G. Apers, Paolo Atzeni, Stefano Ceri, Stefano Paraboschi, Kotagiri Ramamohanarao, and Richard T. Snodgrass, editors. *Proceedings of the Twenty-seventh International Conference on Very Large Data Bases: Roma, Italy, 11–14th September, 2001*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 2001. ISBN 1-55860-804-4. LCCN QA76.9.D3 I559 2001.

Al-Azzoni:2005:MVC

[AADK05] Issam Al-Azzoni, Douglas G. Down, and Ridha Khedri. Modeling and verification of cryptographic protocols using coloured Petri nets and design/CPN. *Nordic Journal of Computing*, 12(3):200–228, Fall 2005. CODEN NJCOFR. ISSN 1236-6064.

Anshel:2001:NKA

[AAFG01] Iris Anshel, Michael Anshel, Benji Fisher, and Dorian Goldfeld. New key agreement protocols in braid group cryptography. *Lecture Notes in Computer Science*, 2020:13–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200013.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200013.pdf.

Almgren:2000:HWC

[AAG+00] Fredrik Almgren, Gunnar Andersson, Torbjörn Granlund, Lars Ivansson, and Staffan Ulfberg. How we cracked the Code Book ciphers. Technical report, ????, ????, October 11, 2000. 40 pp. URL http://frode.home.cern.ch/frode/crypto/codebook_solution.pdf; http://www.simonsingh.com/cipher.htm. See [Sin99].

Ababneh:2009:CSE

[AAK09] Sufyan Ababneh, Rashid Ansari, and Ashfaq Khokhar. Compensated signature embedding for multimedia content authentication. *Journal of Data and Information Quality (JDIQ)*, 1(3):17:1–17:??, December 2009. CODEN ???? ISSN 1936-1955.

Ashraf:2009:SBE

[AAKD09] Manzur Ashraf, Syed Mahfuzul Aziz, M. Lutful Kabir, and Biswajit K. Dey. A SIM-based electronic transaction authentication system. *International Journal of Computer Systems Science and Engineering*, 24 (4):??, July 2009. CODEN CSSEEI. ISSN 0267-6192.

Aamodt:2003:CSP

[Aam03] Ken S. Aamodt. *A cryptographically secure pseudorandom number generator*. Ph.D. thesis, Purdue University, West Lafayette, IN, USA, December 2003. 147 pp. URL http://catalog.lib.purdue.edu/Find/Record/1380784; http://search.proquest.com/docview/305316022?accountid=14677.

Agreste:2007:IAW

[AAPP07] Santa Agreste, Guido Andaloro, Daniela Prestipino, and Luigia Puccio. An image adaptive, wavelet-based watermarking of digital images. *Journal of Computational and Applied Mathematics*, 210(1–2):13–21, December 31, 2007. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042706006431.

An:2001:DER

[AB01] Jee Hea An and Mihir Bellare. Does encryption with redundancy provide authenticity? In *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 512–528. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450512.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450512.pdf.

Atallah:2009:ATC

[AB09] Mikhail J. Atallah and Marina Blanton, editors. *Algorithms and theory of computation handbook. General concepts and techniques*. Chapman and Hall/CRC applied algorithms and data structures series. Chapman and Hall/CRC, Boca Raton, FL, USA, second edition, 2009. ISBN 1-58488-822-9 (print), 1-58488-823-7 (e-book). ???? pp. LCCN QA76.9.A43 A432 2009. URL http://www.crcnetbase.com/isbn/9781584888239.

Abadi:2000:TA

[Aba00] Martín Abadi. Taming the adversary. In Bellare [Bel00], pages 353–??

ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800353.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800353.pdf.

Aiello:2004:JFK

[ABB+04] William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Just fast keying: Key agreement in a hostile Internet. *ACM Transactions on Information and System Security*, 7(2):242–273, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Abdalla:2005:SER

[ABC+05] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In Shoup [Sho05a], pages 205–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Abdalla:2001:DAS

[Abd01] Michel Ferreira Abdalla. *Design and analysis of secure encryption schemes*. Vita thesis (Ph.D.), University of California, San Diego, San Diego, CA, USA, 2001.

Ateniese:2001:ECV

[ABDS01] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. Extended capabilities for visual cryptography. *Theoretical Computer Science*, 250(1–2):143–161, January 6, 2001. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.nl/gej-ng/10/41/16/186/20/29/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/186/20/29/article.pdf.

Abe:2001:SEP

[Abe01] Masayuki Abe. Securing "Encryption + Proof of Knowledge" in the random oracle model. *Lecture Notes in Computer Science*, 2271:277–??, 2001. CO-

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710277.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710277.pdf.

Abe:2004:CEP

[Abe04] Masayuki Abe. Combining encryption and proof of knowledge in the random oracle model. *The Computer Journal*, 47(1): 58–??, January 2004. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_47/Issue_01/470058.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_47/Issue_01/pdf/470058.pdf.

Abadi:2005:CFI

[ABEL05] Martín Abadi, Mihai Budiu, Úlfar Erlingsson, and Jay Ligatti. Control-flow integrity. In Meadows and Syverson [MS05b], pages 340–353. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Adao:2009:SCF

[ABHS09] Pedro Adão, Gergei Bana, Jonathan Herzog, and Andre Scedrov. Soundness and completeness of formal encryption: The cases of key cycles and partial information leakage. *Journal of Computer Security*, 17(5):737–797, ???? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anderson:2000:CS

[ABK00] Ross Anderson, Eli Biham, and Lars Knudsen. The case for Serpent. In NIST [NIS00], pages 349–353. ISBN ???? LCCN ???? URL http://www.cl.cam.ac.uk/ftp/users/rja14/serpentcase.pdf; http://www.cl.cam.ac.uk/ftp/users/rja14/slides-bw.pdf; http://www.cl.cam.ac.uk/ftp/users/rja14/slides.pdf; http://www.cl.cam.ac.uk/~rja14/serpent.html.

Austin:2000:ASF

[ABM00] Todd Austin, Jerome Burke, and John McDonald. Architectural support for fast symmetric-key cryptography. *ACM SIGPLAN Notices*, 35(11):178–189, November 2000. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Adjeroh:2008:BWT

[ABM08] Donald Adjeroh, Tim Bell, and Amar Mukherjee. *The Burrows–Wheeler Transform: Data Compression,* *Suffix Arrays, and Pattern Matching*. Springer Science+Business Media, LLC, Boston, MA, 2008. ISBN 0-387-78908-1, 0-387-78909-X. xxii + 351 pp. LCCN QA76.9.D33 A35 2008.

Abdalla:2001:ODH

[ABR01] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. The oracle Diffie–Hellman assumptions and an analysis of DHIES. *Lecture Notes in Computer Science*, 2020:143–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200143.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200143.pdf.

Ansper:2001:ELT

[ABRW01] Arne Ansper, Ahto Buldas, Meelis Roos, and Jan Willemson. Efficient long-term validation of digital signatures. *Lecture Notes in Computer Science*, 1992:402–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920402.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920402.pdf.

Ambainis:2009:NEQ

[ABW09] Andris Ambainis, Jan Bouda, and Andreas Winter. Nonmalleable encryption of quantum information. *Journal of Mathematical Physics*, 50(4):042106, April 2009. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL http://jmp.aip.org/resource/1/jmapaq/v50/i4/p042106_s1.

Adcock:2002:QGL

[AC02] Mark Adcock and Richard Cleve. A quantum Goldreich–Levin theorem with cryptographic applications. *Lecture Notes in Computer Science*, 2285:323–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2285/22850323.htm; http://link.springer-ny.com/link/service/series/0558/papers/2285/22850323.pdf.

Ateniese:2005:URT

[ACdM05] Giuseppe Ateniese, Jan Camenisch, and Breno de Medeiros. Untraceable RFID tags via insubvertible encryption. In Meadows and

Syverson [MS05b], pages 92–101. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Ateniese:2000:PPS

[ACJT00] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In Bellare [Bel00], pages 255–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800255.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800255.pdf`.

ACM:2000:PTS

[ACM00] ACM, editor. *Proceedings of the thirty second annual ACM Symposium on Theory of Computing: Portland, Oregon, May 21–23, [2000]*. ACM Press, New York, NY 10036, USA, 2000. ISBN 1-58113-184-4. ACM order number 508000.

ACM:2001:PAA

[ACM01a] ACM, editor. *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing: Hersonissos, Crete, Greece, July 6–8, 2001*. ACM Press, New York, NY 10036, USA, 2001. ISBN 1-58113-349-9. LCCN QA76.6 .A13 2001. ACM order number 508010.

ACM:2001:SHP

[ACM01b] ACM, editor. *SC2001: High Performance Networking and Computing. Denver, CO, November 10–16, 2001*. ACM Press and IEEE Computer Society Press, New York, NY 10036, USA and 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2001. ISBN 1-58113-293-X. LCCN ????

ACM:2002:PTF

[ACM02] ACM, editor. *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, Montréal, Québec, Canada, May 19–21, 2002*. ACM Press, New York, NY 10036, USA, 2002. ISBN 1-58113-495-9. LCCN QA75.5 .A22 2002. ACM order number 508020.

ACM:2003:PAS

[ACM03a] ACM, editor. *Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data 2003, San Diego, California, June 09–12, 2003*. ACM Press, New York, NY 10036, USA, 2003. ISBN 1-58113-634-X. LCCN ????

ACM:2003:PTF

[ACM03b] ACM, editor. *Proceedings of the Thirty-Fifth ACM Symposium on Theory of Computing, San Diego, CA, USA, June 9–11, 2003*. ACM Press, New York, NY 10036, USA, 2003. ISBN ???? LCCN QA75.5 .A22 2003. ACM order number 508030.

ACM:2003:PTS

[ACM03c] ACM, editor. *Proceedings of the Twenty-Second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems: PODS 2003: San Diego, Calif., June 9–11, 2003*. ACM Press, New York, NY 10036, USA, 2003. ISBN 1-58113-670-6. LCCN QA76.9.D3 A296 2003. ACM order number 475030.

ACM:2004:PAS

[ACM04a] ACM, editor. *Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data 2004, Paris, France, June 13–18, 2004*. ACM Press, New York, NY 10036, USA, 2004. ISBN 1-58113-859-8. LCCN QA76.9.D3.

ACM:2004:PAA

[ACM04b] ACM, editor. *Proceedings of the 36th Annual ACM Symposium on the Theory of Computing: Chicago, Illinois, USA, June 13–15, 2004*. ACM Press, New York, NY 10036, USA, 2004. ISBN 1-58113-852-0. LCCN QA75.5 .A22 2004.

ACM:2005:MPI

[ACM05a] ACM, editor. *MGC'05: Proceedings of the 3rd International Workshop on Middleware for Grid Computing, Grenoble, France, November 28–December 02, 2005*. ACM Press, New York, NY 10036, USA, 2005. ISBN 1-59593-269-0. LCCN ????

ACM:2005:PTF

[ACM05b] ACM, editor. *Proceedings of the Twenty-Fourth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems: PODS 2005: Baltimore, Maryland, June 13-15, 2005*. ACM Press, New York, NY 10036, USA, 2005. ISBN 1-59593-062-0. LCCN QA76.9.D3 A296 2005. ACM order number 475050.

ACM:2005:SPA

[ACM05c] ACM, editor. *STOC '05: proceedings of the 37th Annual ACM Symposium on Theory of Computing: Baltimore, Maryland, USA, May 22–24, 2005*. ACM Press, New York, NY 10036, USA, 2005. ISBN 1-58113-

960-8. LCCN QA75.5 A22 2005.

ACM:2006:PTE

[ACM06] ACM, editor. *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing 2006, Seattle, WA, USA, May 21–23, 2006*. ACM Press, New York, NY 10036, USA, 2006. ISBN 1-59593-134-1. LCCN QA75.5 .A22 2006. URL http://portal.acm.org/citation.cfm?id=1132516. ACM order number 508060.

ACM:2007:SPA

[ACM07] ACM, editor. *STOC '07: proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11–13, 2007*. ACM Press, New York, NY 10036, USA, 2007. ISBN 1-59593-631-9. LCCN QA75.5 .A22 2007.

ACM:2008:SPA

[ACM08] ACM, editor. *STOC '08: proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17–20, 2008*. ACM Press, New York, NY 10036, USA, 2008. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

ACM:2009:SPA

[ACM09] ACM, editor. *STOC '09: proceedings of the 2009 ACM International Symposium on Theory of Computing, Bethesda, Maryland, USA, May 31–June 2, 2009*. ACM Press, New York, NY 10036, USA, 2009. ISBN 1-60558-613-7. LCCN QA75.5 .A22 2009.

ACM:2010:PAI

[ACM10] ACM, editor. *Proceedings of the 2010 ACM International Symposium on Theory of Computing: June 5–8, 2010, Cambridge, MA, USA*. ACM Press, New York, NY 10036, USA, 2010. ISBN 1-60558-817-2. LCCN QA 76.6 .A152 2010. URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Algesheimer:2002:ECM

[ACS02] Joy Algesheimer, Jan Camenisch, and Victor Shoup. Efficient computation modulo a shared secret with application to the generation of shared safe-prime products. In Yung [Yun02a], pages 417–432. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420417.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420417.pdf.

Alvarez:2005:EBS

[ÁCTZ05] Rafael Álvarez, Joan-Josep Climent, Leandro Tortosa, and Antonio Zamora. An efficient binary sequence generator with cryptographic applications. *Applied Mathematics and Computation*, 167(1):16–27, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300304004709`.

Ahmad:2007:ADE

[AD07] Imtiaz Ahmad and A. Shoba Das. Analysis and detection of errors in implementation of SHA-512 algorithms on FPGAs. *The Computer Journal*, 50(6):728–738, November 2007. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/cgi/content/abstract/50/6/728`; `http://comjnl.oxfordjournals.org/cgi/content/full/50/6/728`; `http://comjnl.oxfordjournals.org/cgi/reprint/50/6/728`.

Anyanwu:2009:DCS

[ADD09] Matthew N. Anyanwu, Lih-Yuan Deng, and Dipankar Dasgupta. Design of cryptographically strong generator by linearly generated sequences. *International Journal of Computer Science and Security (IJCSS)*, 3(3):186–200, June 2009. CODEN ???? ISSN 1985-1553. URL `http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume3/Issue3/IJCSS-78.pdf`.

Avanzi:2006:ESM

[ADDS06] Roberto Avanzi, Vassil Dimitrov, Christophe Doche, and Francesco Sica. Extending scalar multiplication using double bases. *Lecture Notes in Computer Science*, 4284:130–144, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11935230_9.pdf`.

Adee:2009:CDT

[Ade09] S. Adee. Chip design thwarts sneak attack on data. *IEEE Spectrum*, 46(11):16, November 2009. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Arnold:2007:CSE

[ADH+07] T. W. Arnold, A. Dames, M. D. Hocker, M. D. Marik, N. A. Pellicciotti, and K. Werner. Cryptographic system enhancements for the IBM System z9. *IBM Journal of Research and Development*, 51(1/2):87–??, January /March 2007. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL http://www.research.ibm.com/journal/rd/511/arnold.html.

Adikari:2009:HBT

[ADI09] Jithra Adikari, Vassil Dimitrov, and Laurent Imbert. Hybrid binary-ternary joint form and its application in elliptic curve cryptography. In Bruguera et al. [BCDH09], pages 76–83. ISBN 0-7695-3670-0, 1-4244-4329-6. ISSN 1063-6889. LCCN QA76.6 .S887 2009. URL http://www.ac.usc.es/arith19/.

Adleman:2003:TLP

[Adl03] Leonard M. Adleman. Turing Lecture on pre RSA days. World-Wide Web slide presentation, video, and audio., 2003. URL http://www.acm.org/turingawardlecture/RSA/.

An:2002:SJS

[ADR02] Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. *Lecture Notes in Computer Science*, 2332:83–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320083.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320083.pdf.

Arazi:2005:RPK

[AEAQ05] Benjamin Arazi, Itamar Elhanany, Ortal Arazi, and Hairong Qi. Revisiting public-key cryptography for wireless sensor networks. *Computer*, 38(11):103–105, November 2005. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Alvarez:2005:SSS

[AEEdR05] G. Alvarez, A. Hernández Encinas, L. Hernández Encinas, and A. Martín del Rey. A secure scheme to share secret color images. *Computer Physics Communications*, 173(1–2):9–16, December 1, 2005. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465505004224.

Ahmed:2017:IRD

[AEH17] Kareem Ahmed and Ibrahim El-Henawy. Increasing robustness of Data Encryption Standard by integrating DNA cryptography. *International Journal of Computer Applications*, 39(2):91–105, 2017. ISSN 1206-212X (print), 1925-7074 (electronic). URL https:

//www.tandfonline.com/doi/full/10.1080/1206212X.2017.1289690.

Atighehchi:2009:EPA

[AEMR09] Kévin Atighehchi, Adriana Enache, Traian Muntean, and Gabriel Risterucci. An efficient parallel algorithm for Skein hash functions. Report, ERISCS Research Group, Université de la Méditerranée, Parc Scientifique de Luminy-Marseille, France, September 30, 2009. 11 pp.

Anton:2007:HEW

[AEV+07] Annie I. Antón, Julia B. Eart, Matthew W. Vail, Neha Jain, Carrie M. Gheen, and Jack M. Frink. HIPAA's effect on Web site privacy policies. *IEEE Security & Privacy*, 5(1): 45–52, January/February 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Augot:2003:PKE

[AF03] Daniel Augot and Matthieu Finiasz. A public key encryption scheme based on the polynomial reconstruction problem. *Lecture Notes in Computer Science*, 2656: 229–240, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_14.pdf.

Abadi:2004:PA

[AF04a] Martín Abadi and Cédric Fournet. Private authentication. *Theoretical Computer Science*, 322(3):427–476, September 2004. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Abe:2004:ASF

[AF04b] Masayuki Abe and Serge Fehr. Adaptively secure Feldman VSS and applications to universally-composable threshold cryptography. In Franklin [Fra04], pages 317–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Atallah:2005:DEK

[AFB05] Mikhail J. Atallah, Keith B. Frikken, and Marina Blanton. Dynamic and efficient key management for access hierarchies. In Meadows and Syverson [MS05b], pages 190–202. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Ateniese:2006:IPR

[AFGH06] Giuseppe Ateniese, Kevin

Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security*, 9(1):1–30, February 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Attrapadung:2006:FSS

[AFI06] Nuttapong Attrapadung, Jun Furukawa, and Hideki Imai. Forward-secure and searchable broadcast encryption with short ciphertexts and private keys. *Lecture Notes in Computer Science*, 4284:161–177, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11935230_11.pdf.

Akkar:2001:IAS

[AG01] M.-L. Akkar and C. Giraud. An implementation of DES and AES, secure against some attacks. *Lecture Notes in Computer Science*, 2162:309–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620309.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620309.pdf.

Acquisti:2009:PSS

[AG09] Alessandro Acquisti and Ralph Gross. Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences of the United States of America*, 106(27):10975–10980, July 7, 2009. CODEN PNASA6. ISSN 0027-8424 (print), 1091-6490 (electronic). URL http://www.pnas.org/content/early/2009/07/02/0904891106.full.pdf.

Akavia:2006:BOW

[AGGM06] Adi Akavia, Oded Goldreich, Shafi Goldwasser, and Dana Moshkovitz. On basing one-way functions on NP-hardness. In ACM [ACM06], pages 701–710. ISBN 1-59593-134-1. LCCN QA75.5 .A22 2006. URL http://portal.acm.org/citation.cfm?id=1132516. See erratum [AGGM10].

Akavia:2010:EBO

[AGGM10] Adi Akavia, Oded Goldreich, Shafi Goldwasser, and Dana Moshkovitz. Erratum for: *On basing one-way functions on NP-hardness*. In ACM [ACM10], pages 795–796. ISBN 1-60558-817-2. LCCN QA 76.6 .A152 2010. URL http:/

/www.gbv.de/dms/tib-ub-hannover/63314455x.. See [AGGM06].

Alon:2007:GSE

[AGKS07] Noga Alon, Venkatesan Guruswami, Tali Kaufman, and Madhu Sudan. Guessing secrets efficiently via list decoding. *ACM Transactions on Algorithms*, 3 (4):42:1–42:??, November 2007. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Anagnostopoulos:2001:PAD

[AGT01] Aris Anagnostopoulos, Michael T. Goodrich, and Roberto Tamassia. Persistent authenticated dictionaries and their applications. *Lecture Notes in Computer Science*, 2200: 379–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2200/22000379.htm; http://link.springer-ny.com/link/service/series/0558/papers/2200/22000379.pdf.

Ateniese:2005:PRS

[AH05] Giuseppe Ateniese and Susan Hohenberger. Proxy re-signatures: new definitions, algorithms, and applications. In Meadows and Syverson [MS05b], pages 310–319. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Agrawal:2003:SWR

[AHK03a] Rakesh Agrawal, Peter J. Haas, and Jerry Kiernan. A system for watermarking relational databases. In ACM [ACM03a], page 674. ISBN 1-58113-634-X. LCCN ????

Agrawal:2003:WRD

[AHK03b] Rakesh Agrawal, Peter J. Haas, and Jerry Kiernan. Watermarking relational data: framework, algorithms and analysis. *VLDB Journal: Very Large Data Bases*, 12(2):157–169, August 2003. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Armington:2002:BAI

[AHKM02] John Armington, Purdy Ho, Paul Koznek, and Richard Martinez. Biometric authentication in infrastructure security. *Lecture Notes in Computer Science*, 2437:1–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2437/24370001.htm; http://link.springer.de/link/service/series/0558/papers/2437/24370001.pdf.

Ahmad:2007:CSS

[Ahm07] David Ahmad. The contemporary software security landscape. *IEEE Security & Privacy*, 5(3):75–77, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Ahmad:2008:ATT

[Ahm08] David Ahmad. Attack trends: Two years of broken crypto: Debian's dress rehearsal for a global PKI compromise. *IEEE Security & Privacy*, 6(5):70–73, September/October 2008. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Ahmadi:2008:PFS

[AHRH08] O. Ahmadi, D. Hankerson, and F. Rodríguez-Henríquez. Parallel formulations of scalar multiplication on Koblitz curves. *J.UCS: Journal of Universal Computer Science*, 14 (3):481–504, ???? 2008. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_14_3/parallel_formulations_of_scalar.

Askarov:2008:CMF

[AHS08] Aslan Askarov, Daniel Hedin, and Andrei Sabelfeld. Cryptographically-masked flows. *Theoretical Computer Science*, 402(2–3):82–101, August 8, 2008. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Aoki:2001:CBB

[AIK+01] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: a 128-bit block cipher suitable for multiple platforms — design and analysis. *Lecture Notes in Computer Science*, 2012:39–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120039.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120039.pdf.

Applebaum:2004:CNS

[AIK04] B. Applebaum, Y. Ishai, and E. Kushilevitz. Cryptography in NC^0. In IEEE [IEE04], pages 166–175. CODEN ASFPDV. ISBN 0-7695-2228-9. ISSN 0272-5428. LCCN QA276. URL http://ieeexplore.ieee.org/iel5/9430/29918/01366236.pdf?isnumber=29918&prod=CNF&arnumber=1366236&arSt=+166&ared=+175&arAuthor=Applebaum%2C+B.%3B+Ishai%

2C+Y.%3B+Kushilevitz%2C+E.; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=29918&arnumber=1366236&count=64&index=17. IEEE Computer Society Order Number P2228.

Applebaum:2006:C

[AIK06] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. *SIAM Journal on Computing*, 36(4):845–888, ???? 2006. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Al-Ibrahim:2001:AMS

[AIP01] M. Al-Ibrahim and J. Pieprzyk. Authenticating multicast streams in lossy channels using threshold techniques. *Lecture Notes in Computer Science*, 2094: 239–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2094/20940239.htm; http://link.springer-ny.com/link/service/series/0558/papers/2094/20940239.pdf.

Attali:2001:JSC

[AJ01a] Isabelle Attali and Thomas Jensen, editors. *Java on smart cards: programming and security: first international workshop, JavaCard 2000, Cannes, France, September 14, 2000: revised papers*, volume 2041 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-42167-X (paperback). LCCN QA76.73.J38 J3635 2000; QA267.A1 L43 no.2041. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2041.htm. Also available via the World Wide Web.

Attali:2001:SCP

[AJ01b] Isabelle Attali and Thomas Jensen, editors. *Smart card programming and security: International Conference on Research in Smart Cards, E-smart 2001, Cannes, France, September19-21, 2001: proceedings*, volume 2140 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-42610-8 (paperback). LCCN TK7895.S62 I54 2001. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2140.htm.

Aid:2008:NSA

[AJ08] Matthew M. Aid and Thomas R. Johnson. *National Security Agency re-*

leases history of cold war intelligence activities: Soviet strategic forces went on alert three times during September–October 1962 because of apprehension over Cuban situation, top secret codeword history of National Security Agency shows, volume 260 of *National Security Archive electronic briefing book*. National Security Archive, Washington, DC, USA, 2008. LCCN JZ5630. URL http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/index.htm.

Avoine:2008:CIT

[AJO08] Gildas Avoine, Pascal Junod, and Philippe Oechslin. Characterization and improvement of time-memory trade-off based on perfect tables. *ACM Transactions on Information and System Security*, 11(4):17:1–17:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Al-Jarrah:2008:NKM

[AJS08] Omar Al-Jarrah and Ramzy Saifan. A novel key management algorithm in sensor networks. In Gabriele Kotsis et al., editors, *MoMM '08: Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia, 24–26 November 2008, Linz, Austria*, pages 291–294. ACM Press, New York, NY 10036, USA, 2008. ISBN 1-60558-269-7. LCCN QA76.59 .I565 2008.

Abe:2002:KES

[AK02a] Masayuki Abe and Masayuki Kanda. A key escrow scheme with time-limited monitoring for one-way communication. *The Computer Journal*, 45(6):661–671, ???? 2002. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_06/450661.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_06/pdf/450661.pdf.

Agrawal:2002:WRD

[AK02b] Rakesh Agrawal and Jerry Kiernan. Watermarking relational databases. In Bernstein et al. [B+02], pages 155–166. ISBN 1-55860-869-9. LCCN ???? URL http://www.vldb.org/conf/2002/S05P03.pdf.

Armknecht:2003:AAC

[AK03] Frederik Armknecht and Matthias Krause. Algebraic attacks on combiners with memory. In Boneh [Bon03], pages 162–175. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Akinwande:2009:AHC

[Aki09] M. Akinwande. Advances in homomorphic cryptosystems. *J.UCS: Journal of Universal Computer Science*, 15(3):506–??, ???? 2009. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_15_3/advances_in_homomorphic_cryptosystems.

Amir:2004:PGK

[AKNRT04] Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, and Gene Tsudik. On the performance of group key agreement protocols. *ACM Transactions on Information and System Security*, 7 (3):457–488, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Agrawal:2002:PP

[AKS02] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. Report, Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur-208016, India, August 6, 2002. URL http://www.cse.iitk.ac.in/news/primality.pdf.

Aciicmez:2006:PSB

[AKS06] Onur Aciiçmez, Çetin Kaya Koç, and Jean-Pierre Seifert. On the power of simple branch prediction analysis. Technical report, School of EECS, Oregon State University, Corvallis, OR 97331, USA, October 2006. URL http://eprint.iacr.org/2006/351; http://eprint.iacr.org/2006/351.pdf.

Agrawal:2004:OPE

[AKSX04] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Order preserving encryption for numeric data. In ACM [ACM04a], pages 563–574. ISBN 1-58113-859-8. LCCN QA76.9.D3.

Amadio:2000:RPC

[AL00a] Roberto M. Amadio and Denis Lugiez. On the reachability problem in cryptographic protocols. *Lecture Notes in Computer Science*, 1877:380–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/

link/service/series/0558/bibs/1877/18770380.htm; http://link.springer-ny.com/link/service/series/0558/papers/1877/18770380.pdf.

Aoki:2000:FIA

[AL00b] Kazumaro Aoki and Helger Lipmaa. Fast implementations of AES candidates. In NIST [NIS00], pages 106–122. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Atallah:2004:ALA

[AL04] Mikhail J. Atallah and Stefano Lonardi. Augmenting LZ-77 with authentication and integrity assurance capabilities. *Concurrency and Computation: Practice and Experience*, 16(11):1063–1076, September 2004. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Atzeni:2006:PKI

[AL06] Andrea S. Atzeni and Antonio Lioy, editors. *Public Key Infrastructure: Third European PKI Workshop: Theory and Practice, EUROPKI 2006, Turin, Italy, June 19–20, 2006. Proceedings*, volume 4043 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-540-35151-5 (softcover). LCCN ????

Anshel:2007:RME

[AL07] Michael Anshel and Sarah Levitan. Reducing medical errors using secure RFID technology. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 39(2):157–159, June 2007. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). URL https://www.math.utah.edu/pub/mirrors/ftp.ira.uka.de/bibliography/Misc/DBLP/2007.bib.

Allen:2003:EST

[All03] Daniel R. Allen. Eleven SSH tricks. *Linux Journal*, 2003(112):5, August 2003. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Allman:2006:MAW

[All06] Eric Allman. E-mail authentication: what, why, how? *ACM Queue: Tomorrow's Computing Today*, 4 (9):30–34, November 2006. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Alvarez:2000:SMC

[Alv00] David J. Alvarez. *Secret messages: codebreaking and American diplomacy, 1930–1945*. Modern war studies. University Press of Kansas, Lawrence, KS, USA, 2000. ISBN 0-7006-1013-8. xi + 292 pp. LCCN D810.C88 A48 2000. URL http://www.h-net.org/review/hrev-a0b6k4-aa.

Amadio:2002:SRP

[ALV02] Roberto M. Amadio, Denis Lugiez, and Vincent Vanackère. On the symbolic reduction of processes with cryptographic functions. *Theoretical Computer Science*, 290(1):695–740, October 2002. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Abimbola:2006:NSI

[AMB06] A. A. Abimbola, J. M. Munoz, and W. J. Buchanan. NetHost-Sensor: Investigating the capture of end-to-end encrypted intrusive data. *Computers & Security*, 25(6):445–451, September 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404806000605.

Alvarez:2000:CCE

[AMRP00] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of a chaotic encryption system. *Physics Letters A*, 276(1-4):191–196, 2000. CODEN PYLAAG. ISSN 0375-9601 (print), 1873-2429 (electronic).

Alvarez:2004:KCC

[ÁMRP04] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Keystream cryptanalysis of a chaotic cryptographic method. *Computer Physics Communications*, 156(2):205–207, January 1, 2004. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465503004326. See [kWpLwW01, WLW04].

Adams:2007:SAC

[AMW07] Carlisle Adams, Ali Miri, and Michael Wiener, editors. *Selected areas in cryptography: 14th international workshop, SAC 2007, Ottawa, Canada, August 16–17, 2007; revised se-*

lected papers, volume 4876 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-77360-6. LCCN ????

Aljifri:2003:ILA

[AN03] Hassan Aljifri and Diego Sánchez Navarro. International legal aspects of cryptography: Understanding cryptography. *Computers & Security*, 22(3):196–203, April 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404803003055`.

Andem:2003:CTE

[And03] Vikram Reddy Andem. A cryptanalysis of the Tiny Encryption Algorithm. Master of science, Department of Computer Science, The University of Alabama, Tuscaloosa, AL, USA, 2003. viii + 60 pp. URL `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.93.5394`.

Anderson:2004:BRR

[And04] Dennis Anderson. Book review: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* by Klaus Finkenzeller, John Wiley & Sons, 2003, $125, ISBN 0-470-84402-7. *ACM Queue: Tomorrow's Computing Today*, 2(3):74, May 2004. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Anderson:2007:SSS

[And07] Ross Anderson. Software security: State of the art. *IEEE Security & Privacy*, 5(1):8, January/February 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Anderson:2008:MMM

[And08a] M. Anderson. Media: The mash monsters. *IEEE Spectrum*, 45(5):22–23, May 2008. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anderson:2008:SEG

[And08b] Ross Anderson. *Security engineering: a guide to building dependable distributed systems*. John Wiley and Sons, Inc., New York, NY, USA, second edition, 2008. ISBN 0-470-06852-3 (cloth). xl + 1040 pp. LCCN QA76.9.A25 A54 2008. URL `http://www.loc.gov/catdir/enhancements/fy0827/2008006392-d.html`; `http://www.loc.gov/catdir/enhancements/fy0827/2008006392-t.html`.

Aura:2001:RAC

[ANL01] Tuomas Aura, Pekka Nikander, and Jussipekka Leiwo.

DOS-resistant authentication with client puzzles. *Lecture Notes in Computer Science*, 2133: 170–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330170.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330170.pdf.

Anonymous:2000:AIH

[Ano00a] Anonymous. AES IP hardware encryptor introduced. *Network Security*, 2000(9):6–7, September 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348580009019X.

Anonymous:2000:AIah

[Ano00b] Anonymous. Author index. In Bellare [Bel00], pages 545–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/papers/1880/1880auth.pdf.

Anonymous:2000:CRR

[Ano00c] Anonymous. China relaxes rules on encryption products. *Network Security*, 2000 (4):4–5, April 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800040113.

Anonymous:2000:CCI

[Ano00d] Anonymous, editor. *Cool Chips III: An International Symposium on Low-Power and High-Speed Chips, Kikai-Shinko-Kaikan, Tokyo, Japan April 24–25, 2000.* ????, ????, 2000.

Anonymous:2000:CLI

[Ano00e] Anonymous. *Cryptography and liberty 2000: an international survey of encryption policy*. Electronic Privacy Information Center, Washington, DC, USA, 2000. ISBN 1-893044-07-6. iv + 139 pp. LCCN ????

Anonymous:2000:EES

[Ano00f] Anonymous. European encryption still safer than US versions. *Network Security*, 2000(3):3, March 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800030051.

Anonymous:2000:GBE

[Ano00g] Anonymous. Governments back down on encryption regulations. *Net-*

work Security, 2000(5):3–4, May 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348580005008X.

Anonymous:2000:PESa

[Ano00h] Anonymous. PGP encryption software granted global export license. *Network Security*, 2000(1):1, January 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800900242.

Anonymous:2000:PTD

[Ano00i] Anonymous. Privacy threatened by digital signatures. *Network Security*, 2000(5):4, May 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800050091.

Anonymous:2000:SES

[Ano00j] Anonymous. Signing and encryption software system launched. *Network Security*, 2000(5):6, May 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800050170.

Anonymous:2000:UAS

[Ano00k] Anonymous. User authentication via smart card. *Network Security*, 2000(9):7, September 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800090206.

Anonymous:2000:VAS

[Ano00l] Anonymous. Voice authentication smart card. *Network Security*, 2000(10):5, October 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800100145.

Anonymous:2001:AAPb

[Ano01a] Anonymous. An anonymous auction protocol using “money escrow” (transcript of discussion). *Lecture Notes in Computer Science*, 2133:223–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330223.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330223.pdf.

Anonymous:2001:ANT

[Ano01b] Anonymous. Authentication and naming (transcript of discussion). *Lecture Notes in Computer Science*, 2133:20–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330020.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330020.pdf.

Anonymous:2001:AWB

[Ano01c] Anonymous. Authentication Web-based virtual shops using signature-embedded marks — A practical analysis — (transcript of discussion). *Lecture Notes in Computer Science*, 2133:249–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330249.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330249.pdf.

Anonymous:2001:AIgb

[Ano01d] Anonymous. Author index. In Kilian [Kil01a], pages 599–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/papers/2139/2139auth.pdf.

Anonymous:2001:CCA

[Ano01e] Anonymous. Censoring crypto not the answer says Schneier. *Network Security*, 2001(10):4, October 31, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348580101011X.

Anonymous:2001:RAC

[Ano01f] Anonymous. DOS-resistant authentication with client puzzles (transcript of discussion). *Lecture Notes in Computer Science*, 2133:178–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330178.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330178.pdf.

Anonymous:2001:EDS

[Ano01g] Anonymous. Encryption and digital signature standards. Technical report AD-a398 639, National Aeronautics and Space Administration, Ames Research Center, Moffett Field, CA, USA, 2001. 14 pp.

Anonymous:2001:EER

[Ano01h] Anonymous. Encryption expert released on bail. *Network Security*, 2001(8):2, August 1, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485801008029.

Anonymous:2001:EMB

[Ano01i] Anonymous. Encryption market bolstered by hackers. *Network Security*, 2001 (7):4, July 1, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485801007115.

Anonymous:2001:LBS

[Ano01j] Anonymous. Looking on the bright side of black-box cryptography (transcript of discussion). *Lecture Notes in Computer Science*, 2133:54–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330054.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330054.pdf.

Anonymous:2001:MLF

[Ano01k] Anonymous. Magic Lantern fries crypto keys. *Network Security*, 2001(12):2, December 1, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485801012028.

Anonymous:2001:MIT

[Ano01l] Anonymous. Massive identity theft by NY dish washer. *Network Security*, 2001(4):2, April 1, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485801004020.

Anonymous:2001:NWS

[Ano01m] Anonymous. Netherlands to watch strong crypto. *Network Security*, 2001(10):4, October 31, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485801010121.

Anonymous:2001:PKC

[Ano01n] Anonymous. Public-key crypto-systems using symmetric-key crypto-algorithms (transcript of discussion). *Lecture Notes in Computer Science*, 2133:184–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330184.htm;

http://link.springer-ny.com/link/service/series/0558/papers/2133/21330184.pdf.

Anonymous:2001:SCS

[Ano01o] Anonymous. Short certification of secure RSA modulus (transcript of discussion). *Lecture Notes in Computer Science*, 2133: 234–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330234.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330234.pdf.

Anonymous:2001:TAD

[Ano01p] Anonymous. Talking about digital copyright. *IEEE Spectrum*, 38(6):9, June 2001. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:2002:DEC

[Ano02a] Anonymous. *Data encryption and cryptography*. Academia Sinica, Institute of Information Science, Taipei, 2002. ISSN 1016-2364. i–ii, 349–391 pp. JISE J. Inf. Sci. Eng. **18** (2002), no. 3.

Anonymous:2002:IHB

[Ano02b] Anonymous. The importance of hardware-based cryptography for added security. *Network Security*, 2002(3):5, March 31, 2002. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485802003069.

Anonymous:2002:NSD

[Ano02c] Anonymous. NASA secret data hacked. *Network Security*, 2002(9):2–3, September 1, 2002. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485802090025.

Anonymous:2002:PPD

[Ano02d] Anonymous. Products: Palm Digital Media's eBook publishing tools; Veridicom's fingerprint authentication module; high-speed debugging tool for Macraigor Systems; QNX launches IDE for embedded programming; Extreme Networks' network management tools; Parascript's handwriting recognition SDK; system debugger tool from Compuware. *Computer*, 35(8):74–??, August 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/dl/mags/co/2002/08/r8074.htm; http://csdl.computer.

org/dl/mags/co/2002/08/r8074.pdf.

Anonymous:2002:PSS

[Ano02e] Anonymous. Products: SOISIC ships design kit for SOI structures; systems and software development tools from Telelogic; RSA Security's Web access management system; Altera's free embedded processor portfolio; signal integrity measurement tools from Tektronix; Oracle upgrades Java development tool; Xilinx delivers EDK for FPGA processor; Westbridge's tool to sniff unauthorized XML; SpeechStudio's telephony development tools. *Computer*, 35(12):118–119, December 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/dl/mags/co/2002/12/rz118.htm; http://csdl.computer.org/dl/mags/co/2002/12/rz118.pdf.

Anonymous:2002:PFQ

[Ano02f] Anonymous. Promise from the future — quantum cryptography. *Network Security*, 2002(9):6, September 1, 2002. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485802090074.

Anonymous:2002:QCQ

[Ano02g] Anonymous, editor. *Quantum computation and quantum cryptography*, volume 34(4) of *Algorithmica*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). 309–559 pp.

Anonymous:2002:QCR

[Ano02h] Anonymous. Quantum cryptography revisited. *Network Security*, 2002(8):14–16, August 1, 2002. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485802080121.

Anonymous:2002:RUB

[Ano02i] Anonymous. Review of US bombes. *IEEE Annals of the History of Computing*, 24(3):85–87, July–September 2002. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL http://computer.org/annals/an2002/a3letter_web/a3lettertoeditor_web.htm; http://dlib.computer.org/an/books/an2002/pdf/a3085.pdf; http://www.computer.org/annals/an2002/a3085abs.htm.

Anonymous:2003:TMC

[Ano03a] Anonymous. For Taiwan's 22 million citizens, Java Smart Cards are clamping down on health-care fraud. *PC Magazine*, 22(17):66–67, 2003. CODEN PCMGEP. ISSN 0888-8507.

Anonymous:2003:YCS

[Ano03b] Anonymous. Is your current security SECURE?: John Jessop, Cryptic Software. *Network Security*, 2003(4): 3, April 2003. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485803004069.

Anonymous:2003:NAW

[Ano03c] Anonymous. Network armies in a world without secrets. *Network Security*, 2003(3):14–15, March 2003. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485803003118.

Anonymous:2003:NUP

[Ano03d] Anonymous. News 2.0: Uncrackable passwords; WebFountain drinks down the Web; embracing open source in India. *ACM Queue: Tomorrow's Computing Today*, 1(5):8, July/August 2003. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Anonymous:2003:SEY

[Ano03e] Anonymous. Secret enough for you? *IEEE Spectrum*, 40 (4):9, April 2003. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:2003:TMP

[Ano03f] Anonymous. Table of Mersenne primes, 2003. URL http://mathworld.wolfram.com/MersennePrime.html; http://primes.utm.edu/mersenne/; http://primes.utm.edu/top20/page.php?id=4; http://www.computerworld.com/s/article/9236570/Mathematician_Finding_17M_digit_prime_number_like_climbing_Everest; http://www.mersenne.org/; http://www.mersenne.org/prime.htm; http://www.mersenne.org/report_milestones/; http://www.mersenne.org/various/57885161.htm; http://www.perfsci.com/wall-art.asp; http://www.utm.edu/research/primes/mersenne/index.html; http://www.utm.edu/research/primes/notes/3021377/. Mersenne primes are primes of the form $M(n) = 2^p - 1$. The known members of this set in order of increasing p (not of discovery), year of discov-

ery, and discoverer, are:

n	*p*	**year**	**discoverer**
1	2	unknown	unknown
2	3	unknown	unknown
3	5	unknown	unknown
4	7	unknown	unknown
5	13	1461	Anonymous
6	17	1588	P. A. Cataldi
7	19	1588	P. A. Cataldi
8	31	1750	L. Euler
9	61	1883	I. M. Pervushin
10	89	1911	R. E. Powers
11	107	1913	E. Fauquembergue
12	127	1876	E. Lucas
13	521	1952	R. M. Robinson
14	607	1952	R. M. Robinson
15	1279	1952	R. M. Robinson
16	2203	1952	R. M. Robinson
17	2281	1952	R. M. Robinson
18	3217	1957	H. Riesel
19	4253	1961	A. Hurwitz
20	4423	1961	A. Hurwitz
21	9689	1963	D. B. Gillies
22	9941	1963	D. B. Gillies
23	11213	1963	D. B. Gillies
24	19937	1971	B. Tuckerman
25	21701	1978	L. C. Noll & L. Nickel
26	23209	1979	L. C. Noll
27	44497	1979	H. Nelson & D. Slowinski
28	86243	1982	D. Slowinski
29	110503	1988	W. N. Colquitt & L. Welsch, Jr.
30	132049	1983	D. Slowinski
31	216091	1985	D. Slowinski
32	756839	1992	Slowinski & Gage
33	859433	1994	Slowinski & Gage
34	1257787	1996	Slowinski & Gage
35	1398269	1996	Armengaud et al. (GIMPS)
36	2976221	1997	Spence et al. (GIMPS)
37	3021377	1998	Clarkson, Woltman, Kurowski, and Slowinski (GIMPS)
38	6972593	1999	Hajratwala et al. (GIMPS)
39	13466917	2001	M. Cameron (GIMPS)
40	20996011	2003	M. Shafer (GIMPS)
41	24036583	2004	Josh Findley (GIMPS)
42	25964951	2005	Martin Nowak (GIMPS)
43	30402457	2005	Curtis Cooper & Steven Boone (GIMPS)
44	32582657	2006	Curtis Cooper & Steven Boone (GIMPS)
45	37156667	2008	Hans-Michael Elvenich, George Woltman, Scott Kurowski (GIMPS)
46	42643801	2009	Odd Magnar Strindmo (GIMPS)
47	43112609	2008	Edson Smith, George Woltman, Scott Kurowski (GIMPS)
48	57885161	2013	Curtis Cooper, George Woltman, Scott Kurowski, and others
49	74207281	2016	Curtis Cooper (GIMPS)
50	77232917	2017	Jon Pace (GIMPS)
51 (??)	82589933	2018	P. Laroche, G. Woltman, A. Blosser, et al. (GIMPS)

Anonymous:2003:UCD

[Ano03g] Anonymous. Unravelling crypto developments: Dr Nicko van Someren, founder and CTO of nCipher, sorts out fact from fiction when it comes to quantum encryption. *Network Security*, 2003(9):7–8, September 2003. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485803009061.

Anonymous:2004:BB

[Ano04a] Anonymous. Biometrics boom. *IEEE Spectrum*, 41 (3):13, March 2004. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:2004:CPS

[Ano04b] Anonymous. Call for papers for special section on fault diagnosis and tolerance in cryptography. *IEEE Transactions on Computers*, 53 (11):1504, November 2004. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1336771.

Anonymous:2004:CJL

[Ano04c] Anonymous. Chipkarten: Java-Lösung für SmartCards. (German) [Chip cards: Java solutions for SmartCards]. *Elektronik*, 53(4):6, 2004. CODEN EKRKAR. ISSN 0013-5658.

Anonymous:2004:Cf

[Ano04d] Anonymous. Codebuster. *IEEE Spectrum*, 41(5):59–60, May 2004. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:2004:ISL

[Ano04e] Anonymous. IBM's support for the Liberty Alliance brings standard convergence for federated identity a step closer. *Network Security*, 2004(11):3, 20, November 2004. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485804001515.

Anonymous:2004:NGJ

[Ano04f] Anonymous. New generation Java smart cards. *Card Technology Today*, 16(3):10–11, 2004. CODEN ???? ISSN 0965-2590.

Anonymous:2005:CEC

[Ano05a] Anonymous. The case for elliptic curve cryptography. US National Security Agency World-Wide Web document, October 2005. URL http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm.

Anonymous:2005:SCB

[Ano05b] Anonymous. Smart card based authentication — any future? *Computers & Security*, 24(3):188–191, May 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S016740480500043X.

Anonymous:2005:WAS

[Ano05c] Anonymous. Workshop on architectural support for security and anti-virus (WASSA). *ACM SIGARCH Computer Architecture News*, 33(1):??, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Anonymous:2006:JHD

[Ano06a] Anonymous. Just 12% of handheld devices encrypted. *Network Security*, 2006(7):20, July 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485806704159.

Anonymous:2006:RC

[Ano06b] Anonymous. RSA(R) Conference 2007. *IEEE Security & Privacy*, 4(6):14, November/December 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Anonymous:2006:SSD

[Ano06c] Anonymous. *Solaris Security for Developers Guide*. Sun Microsystems, 2550 Garcia Avenue, Mountain View, CA 94043, USA, 2006. ISBN 0-595-28558-9. ???? pp. LCCN ???? URL http://docs.sun.com/app/docs/doc/816-4863.

Anonymous:2006:SQE

[Ano06d] Anonymous. Success for quantum encryption? *Network Security*, 2006(5):20, May 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485806703920.

Anonymous:2007:CPSh

[Ano07a] Anonymous. Call for papers for special section on special-purpose hardware for cryptography and cryptanalysis. *IEEE Transactions on Computers*, 56(10):1439, October 2007. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Anonymous:2007:CPSf

[Ano07b] Anonymous. Call for papers: Special-purpose hardware for cryptography and cryptanalysis. *IEEE Transactions on Computers*, 56(7):1008, July 2007. CODEN ITCOB4. ISSN 0018-

9340 (print), 1557-9956 (electronic).

Anonymous:2008:KAD

[Ano08a] Anonymous. Kaspersky asks for decryption help. *Network Security*, 2008(7): 1–2, July 2008. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485808700813.

Anonymous:2008:RCB

[Ano08b] Anonymous. Researchers crack bot net secrets. *Network Security*, 2008(5): 2, May 2008. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485808700588.

Anonymous:2008:RES

[Ano08c] Anonymous. Researchers encode secret messages in VoIP calls. *Network Security*, 2008(7): 2, July 2008. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485808700837.

Anonymous:2008:SHS

[Ano08d] Anonymous. Secure Hash Standard (SHS). Federal Information Processing Standards Publication FIPS Pub 180-3, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, October 2008. v + 27 pp. URL http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf. Superceded by FIPS 180-4 [Ano12].

Anonymous:2009:BG

[Ano09a] Anonymous. Breaking gsm. *IEEE Spectrum*, 46(12):13, December 2009. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:2009:DSS

[Ano09b] Anonymous. Digital Signature Standard (DSS). Federal Information Processing Standards Publication FIPS Pub 186-3, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, June 2009. ix + 119 pp. URL http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf. Superceded by FIPS 186-4 [Ano13].

Anonymous:2009:PCA

[Ano09c] Anonymous. Proof of concept attack further discredits MD5. *Network Security*, 2009(1):2, January 2009. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S1353485809700030.

Anonymous:2009:TCA

[Ano09d] Anonymous. The transitioning of cryptographic algorithms and key sizes. Web document, July 2, 2009. URL https://csrc.nist.gov/csrc/media/projects/key-management/documents/transitions/transitioning_cryptoalgos_070209.pdf.

Anonymous:2012:SHS

[Ano12] Anonymous. Secure Hash Standard (SHS). Federal Information Processing Standards Publication FIPS Pub 180-4, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, March 2012. v + 30 pp. URL http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf; http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4.

Anonymous:2013:DSS

[Ano13] Anonymous. Digital Signature Standard (DSS). Federal Information Processing Standards Publication FIPS Pub 186-4, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, July 2013. vii + 121 pp. URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

Ateniese:2001:SRC

[ANR01] Giuseppe Ateniese and Cristina Nita-Rotaru. Stateless-recipient certified E-mail system based on verifiable encryption. *Lecture Notes in Computer Science*, 2271:182–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710182.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710182.pdf.

Amir:2001:FAA

[ANRS01] Yair Amir, Cristina Nita-Rotaru, and Jonathan R. Stanton. Framework for authentication and access control of client-server group communication systems. *Lecture Notes in Computer Science*, 2233:128–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2233/22330128.htm; http://link.springer-ny.com/link/service/series/0558/papers/2233/22330128.pdf.

ANSI:2005:AXP

[ANS05] ANSI. *ANSI X9.62:2005: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, 2005. URL http://csrc.nist.gov/encryption/dss/ecdsa/NISTReCur.pdf; http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9%2E62%3A2005.

Abe:2000:PSP

[AO00] Masayuki Abe and Tatsuaki Okamoto. Provably secure partially blind signatures. In Bellare [Bel00], pages 271–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800271.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800271.pdf.

Abe:2002:SVK

[AOS02] Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. *Lecture Notes in Computer Science*, 2501: 415–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010415.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010415.pdf.

Alomair:2009:ITS

[AP09] B. Alomair and R. Poovendran. Information theoretically secure encryption with almost free authentication. *J.UCS: Journal of Universal Computer Science*, 15(15):2937–??, ???? 2009. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_15_15/information_theoretically_secure_encryption.

Appenzeller:2005:IBE

[App05] Guido Appenzeller. Identity-based encryption from algorithm to enterprise deployment. In Meadows and Syverson [MS05b], page 406. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Applebaum:2007:CCP

[App07] Benny Applebaum. *Cryptography in Constant Parallel Time*. Ph.D. dissertation, Technion — Israel Institute of Technology, Haifa, Israel, 2007. URL http://www.acm.org/press-room/news-releases/dd-award-07. Honorable Mention for the ACM 2007 Doctoral Dissertation Award.

Alwen:2005:IFR

[APV05] Joë Alwen, Giuseppe Persiano, and Ivan Visconti. Impossibility and feasibility results for zero knowledge with public keys. In Shoup [Sho05a], pages 135–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Abdalla:2000:NFS

[AR00] Michel Abdalla and Leonid Reyzin. A new forward-secure digital signature scheme. *Lecture Notes in Computer Science*, 1976: 116–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760116.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760116.pdf.

Arboit:2001:FLM

[AR01] Geneviève Arboit and Jean-Marc Robert. From fixed-length messages to arbitrary-length messages practical RSA signature padding schemes. *Lecture Notes in Computer Science*, 2020:44–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200044.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200044.pdf.

Araki:2002:NRS

[Ara02] Shunsuke Araki. A Nyberg–Rueppel signature for multiple messages and its batch verification. *Lecture Notes in Computer Science*, 2433: 220–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330220.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330220.pdf.

Atallah:2001:NLW

[ARC+01] Mikhail J. Atallah, Victor Raskin, Michael Crogan, Christian Hempelmann, Florian Kerschbaum, Dina Mohamed, and Sanket Naik. Natural language watermarking: Design, analysis, and a proof-of-concept implementation. *Lecture Notes in Computer Science*, 2137:185–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370185.htm; http://link.springer-ny.com/link/service/series/0558/papers/2137/21370185.pdf.

Aaraj:2008:ADH

[ARJ08] Najwa Aaraj, Anand Raghunathan, and Niraj K. Jha. Analysis and design of a hardware/software trusted platform module for embedded systems. *ACM Transactions on Embedded Computing Systems*, 8(1):8:1–8:??, December 2008. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Arkin:2005:CND

[Ark05] William M. Arkin. *Code names: deciphering US military plans, programs, and operations in the 9/11 world*. Steerforth Press, Hanover, NH, USA, 2005. ISBN 1-58642-083-6. 608 pp. LCCN UA23 .A689 2005. URL http://www.loc.gov/catdir/toc/ecip052/2004025039.html.

Arnold:2001:AWB

[Arn01] Michael Arnold. Audio watermarking: Burying information in the data. *Dr. Dobb's Journal of Software Tools*, 26(11):21–22, 24–26, 28, November 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ftp/2001/2001_11/watermk.txt; http://www.ddj.com/ftp/2001/2001_11/watermk.zip.

Agrawal:2003:MCA

[ARR03] Dakshi Agrawal, Josyula R. Rao, and Pankaj Rohatgi. Multi-channel attacks. In Walter et al. [WKP03], pages 2–16. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Artail:2004:PAC

[Art04] Hassan A. Artail. Peer-assisted carrying authentication (PACA). *Computers & Security*, 23(6):478–488, September 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001191.

Abe:2001:SPA

[AS01a] Masayuki Abe and Koutarou Suzuki. $M + 1$-st price auction using homomorphic encryption. *Lecture Notes in Computer Science*, 2274:115–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740115.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740115.pdf.

Adelsbach:2001:ZKW

[AS01b] André Adelsbach and Ahmad-Reza Sadeghi. Zero-knowledge watermark detection and proof of ownership. *Lecture Notes in Computer Science*, 2137:273–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370273.htm; http://link.springer-ny.com/link/service/series/0558/papers/2137/21370273.pdf.

Agung:2001:ICI

[AS01c] I. Wiseto Agung and Peter Sweeney. Improvement and comments on image watermarking using complementary modulation. *Lecture Notes in Computer Science*, 2195:411–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950411.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950411.pdf.

Agarwal:2008:DWS

[AS08] Rashmi Agarwal and M. S. Santhanam. Digital watermarking in the singular vector domain. *International Journal of Image and Graphics (IJIG)*, 8(3):351–368, July 2008. CODEN ???? ISSN 0219-4678.

Asenjo:2002:AES

[Ase02] Juan C. Asenjo. The Advanced Encryption Standard — implementation and transition to a new cryptographic benchmark. *Network Security*, 2002(7):7–9, July 1, 2002. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485802070083.

Ashburn:2003:PBA

[Ash03] Julian Ashburn. *Practical Biometrics: From*

Aspiration to Implementation. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 1-85233-774-5. xiv + 159 pp. LCCN TK7882.B56A84 2003. US$49.95.

Aciicmez:2005:IBB

[ASK05] Onur Aciiçmez, Werner Schindler, and Çetin K. Koç. Improving Brumley and Boneh timing attack on unprotected SSL implementations. In Meadows and Syverson [MS05b], pages 139–146. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Aciicmez:2007:MAC

[ASK07] Onur Aciiçmez, Jean-Pierre Seifert, and Çetin Kaya Koç. Micro-architectural cryptanalysis. *IEEE Security & Privacy*, 5(4):62–64, July/August 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Aslan:2004:HSM

[Asl04a] Heba K. Aslan. A hybrid scheme for multicast authentication over lossy networks. *Computers & Security*, 23(8):705–713, December 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001798.

Aslan:2004:LAA

[Asl04b] Heba K. Aslan. Logical analysis of AUTHMAC_DH: a new protocol for authentication and key distribution. *Computers & Security*, 23 (4):290–299, June 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804000215.

Blanchet-Sadri:2001:MSD

[aSM01] F. Bl anchet Sadri and C. Morgan. Multiset and set decipherable codes. *Computers and Mathematics with Applications*, 41 (10–11):1257–1262, May/June 2001. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122101000967.

Abdalla:2000:KMR

[ASW00] Michel Abdalla, Yuval Shavitt, and Avishai Wool. Key management for restricted multicast using broadcast encryption. *IEEE/ACM Transactions on Networking*, 8(4):443–454, 2000. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL http://www.acm.org/pubs/citations/journals/ton/2000-8-4/p443-abdalla/.

Allison:2001:LLE

[ASW+01] Dennis Allison, Randy Schrickel, Reid Womack, Jeremy C. Reed, Ashley Tate, and Paul Munsey. Letters: Looking for early PPC [People's Computing Company] people; being prepared for invasion; BetterBASIC; Linux versus BSD; Diffie–Hellman to the rescue; the future of programming. *Dr. Dobb's Journal of Software Tools*, 26 (6):10, 12, June 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Ateniese:2004:VED

[Ate04] Giuseppe Ateniese. Verifiable encryption of digital signatures and applications. *ACM Transactions on Information and System Security*, 7(1):1–20, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Androutsellis-Theotokis:2004:SPP

[ATS04] Stephanos Androutsellis-Theotokis and Diomidis Spinellis. A survey of peer-to-peer content distribution technologies. *ACM Computing Surveys*, 36(4):335–371, December 2004. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Aharonov:2000:QBE

[ATSVY00] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In ACM [ACM00], pages 705–714. ISBN 1-58113-184-4. URL http://www.acm.org/pubs/articles/proceedings/stoc/335305/p705-aharonov/p705-aharonov.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/335305/p705-aharonov/. ACM order number 508000.

Alster:2001:PKC

[AUW01] Kazimierz Alster, Jerzy Urbanowicz, and Hugh C. Williams, editors. *Public-key cryptography and computational number theory: proceedings of the international conference organized by the Stefan Banach International Mathematical Center, Warsaw, Poland, September 11-15, 2000*. Walter de Gruyter, New York, NY, USA, 2001. ISBN 3-11-017046-9 (cloth). LCCN QA268 .P83 2001.

Arnold:2004:IPN

[AV04] T. W. Arnold and L. P. Van Doorn. The IBM PCIXCC: a new cryptographic coprocessor for the IBM eServer. *IBM Journal of Research and Development*, 48(3/4): 475–487, ???? 2004. CODEN IBMJAE. ISSN 0018-

8646 (print), 2151-8556 (electronic). URL http://www.research.ibm.com/journal/rd/483/arnold.html; http://www.research.ibm.com/journal/rd/483/arnold.pdf.

Avanzi:2003:CAD

[Ava03] Roberto M. Avanzi. Countermeasures against differential power analysis for hyperelliptic curve cryptosystems. In Walter et al. [WKP03], pages 366–381. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Aalberts:2000:DSB

[AvdH00] Babette Aalberts and Simone van der Hof. *Digital signature blindness: analysis of legislative approaches toward electronic authentication*. Number 32 in ITeR, Nationaal programma informatietechnologie en recht. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2000. ISBN 90-268-3656-2. 77 pp. LCCN K564.C6 A73 2000. In English with summary in Dutch.

Abadi:2005:SAC

[AW05] Martín Abadi and Bogdan Warinschi. Security analysis of cryptographically controlled access to XML documents. In ACM [ACM05b], pages 108–117. ISBN 1-59593-062-0. LCCN QA76.9.D3 A296 2005. ACM order number 475050.

Abadi:2008:SAC

[AW08] Martín Abadi and Bogdan Warinschi. Security analysis of cryptographically controlled access to XML documents. *Journal of the ACM*, 55(2):6:1–6:29, May 2008. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Ayoade:2006:SIR

[Ayo06] John Ayoade. Security implications in RFID and authentication processing framework. *Computers & Security*, 25(3):207–212, May 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404805001951.

Bernstein:2002:VPT

[B+02] Philip A. Bernstein et al., editors. *VLDP 2002: pro-*

ceedings of the Twenty-Eighth International Conference on Very Large Data Bases, Hong Kong SAR, China, 20–23 August 2002. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 2002. ISBN 1-55860-869-9. LCCN ????

Blanton:2006:SRF

[BA06] Marina Blanton and Mikhail Atallah. Succinct representation of flexible and privacy-preserving access rights. *VLDB Journal: Very Large Data Bases*, 15(4): 334–354, November 2006. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Bagnulo:2002:PAA

[BACS02] Marcelo Bagnulo, Bernardo Alarcos, María Calderón, and Marifeli Sedano. Providing authentication & authorization mechanisms for active service charging. *Lecture Notes in Computer Science*, 2511: 337–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2511/25110337.htm; http://link.springer.de/link/service/series/0558/papers/2511/25110337.pdf.

Badra:2007:AWC

[Bad07] Mohamad Badra. Alternative wireless client authentication and key distribution. *Network Security*, 2007(7): 9–13, July 2007. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485807700648.

Baier:2001:ECP

[Bai01a] H. Baier. Elliptic curves of prime order over optimal extension fields for use in cryptography. *Lecture Notes in Computer Science*, 2247:99–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470099.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470099.pdf.

Baier:2001:ECS

[Bai01b] Harald Baier. Efficient computation of singular moduli with application in cryptography. *Lecture Notes in Computer Science*, 2138: 71–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2138/21380071.htm; http://link.springer-ny.com/link/service/series/

0558/papers/2138/21380071.pdf.

Baigneres:2008:QSB

[Bai08] Thomas Baignères. *Quantitative security of block ciphers : designs and cryptanalysis tools*. Thèse, Faculté informatique et communications IC, Programme doctoral Informatique, Communications et Information, Institut de systèmes de communication ISC (Laboratoire de sécurité et de cryptographie LASEC), École polytechnique fédérale de Lausanne EPFL, Lausanne, Switzerland, 2008. 243 pp.

Bamford:2002:BSA

[Bam02] James Bamford. *Body of secrets: anatomy of the ultra-secret National Security Agency*. Anchor Books, New York, NY, USA, 2002. ISBN 0-385-49908-6. 763 pp. LCCN UB256.U6 B36 2002. URL http://www.loc.gov/catdir/bios/random051/2002284054.html; http://www.loc.gov/catdir/description/random043/2002284054.html; http://www.loc.gov/catdir/samples/random041/2002284054.html.

Banks:2005:TFC

[Ban05] William D. Banks. Towards faster cryptosystems, II. In Garrett and Lieman [GL05], pages 139–152. ISBN 0-8218-3365-0. LCCN QA76.9.A25 P82 2005. URL http://www.loc.gov/catdir/toc/fy0612/2005048178.html.

Bao:2004:CPK

[Bao04] Feng Bao. Cryptanalysis of a partially known cellular automata cryptosystem. *IEEE Transactions on Computers*, 53(11):1493–1497, November 2004. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1336769.

Baran:2000:NVB

[Bar00a] Nicholas Baran. News and views: 108-bit elliptic curve cryptographic key found; new algorithm cracks the stock market; first complete Babbage printer unveiled; XrML view to be digital rights standard; PKWare founder [phil katz] dies unexpectedly. *Dr. Dobb's Journal of Software Tools*, 25(7):18, July 2000. CODEN DDJOEB. ISSN 1044-789X.

Baran:2000:NVM

[Bar00b] Nicholas Baran. News and views: More on tiny transistors; Open Source repository launched; design contest promotes new software tools; and then there's a decryption contest; Fred

Brooks wins ACM Turing Award. *Dr. Dobb's Journal of Software Tools*, 25 (3):18, March 2000. CODEN DDJOEB. ISSN 1044-789X. URL http://sourceforge.net/.

Baran:2000:NVR

[Bar00c] Nicholas Baran. News and views: RSA algorithm in the public domain; Woz joins the Inventors Hall of Fame; entangled photons mean faster, smaller ICs; BEHEMOTH mothballed; Advanced Encryption Standard selected; SGI releases SDK as open source; WSDL spec released. *Dr. Dobb's Journal of Software Tools*, 25(12):18, December 2000. CODEN DDJOEB. ISSN 1044-789X.

Barr:2002:IC

[Bar02] Thomas H. Barr. *Invitation to Cryptology*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 2002. ISBN 0-13-088976-8. xii + 396 pp. LCCN Z103 .B34 2002.

Barken:2003:HSY

[Bar03] Lee Barken. *How Secure is Your Wireless Network? Safeguarding Your Wi-Fi LAN*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 2003. ISBN 0-13-140206-4. xx + 199 pp. LCCN QA76.9.A25B3775 2003. US$34.99.

Barron:2005:DWP

[Bar05] David W. Barron. David Wheeler: a personal memoir. *The Computer Journal*, 48(6):650–651, November 2005. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/full/48/6/650; http://comjnl.oxfordjournals.org/cgi/reprint/48/6/650.

Barkan:2006:CCP

[Bar06a] Elad Pinhas Barkan. *Cryptanalysis of ciphers and protocols*. Thesis (Ph.D.), Faculty of Computer Science, Technion — Israel Institute of Technology, Haifa, Israel, 2006. vi + 176 pp.

Barker:2006:ROA

[Bar06b] Elaine Barker. *Recommendation for Obtaining Assurances for Digital Signature Applications*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, November 2006. v + 33 pp. URL http://csrc.nist.gov/CryptoToolkit/dss/SP800-89Nov2006.pdf. NIST Special Publication 800-89.

Bard:2009:AC

[Bar09] Gregory V. Bard. *Algebraic cryptanalysis*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 0-387-88757-1 (ebook), 0-387-88756-3. xxxiii + 356 pp. LCCN Z103 .B37 2009eb. URL http://link.library.utoronto.ca/eir/EIRdetail.cfm?Resources__ID=896123&T=F.

Bauer:2000:DSM

[Bau00] Friedrich Ludwig Bauer. *Decrypted secrets: methods and maxims of cryptology*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2000. ISBN 3-540-66871-3. xii + 470 pp. LCCN QA76.9.A25 B38513 2000.

Bauer:2001:PPGa

[Bau01a] Mick Bauer. Paranoid penguin GPG: The best free crypto you aren't using, Part I of II. *Linux Journal*, 89:32–34, 36–37, September 2001. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://noframes.linuxjournal.com/lj-issues/issue89/4828.html.

Bauer:2001:PPGb

[Bau01b] Mick Bauer. Paranoid penguin: GPG: the best free crypto you aren't using, Part II of II. *Linux Journal*, 90:46, 48, 50–52, 54–55, October 2001. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Bauer:2001:PPUb

[Bau01c] Mick Bauer. Paranoid penguin: The 101 uses of OpenSSH: Part II of II. *Linux Journal*, 82:52, 54, 56, 58–59, February 2001. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Bauer:2002:DSM

[Bau02a] Friedrich Ludwig Bauer. *Decrypted secrets: methods and maxims of cryptology*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., third edition, 2002. ISBN 3-540-42674-4. xii + 473 pp. LCCN QA76.9.A25 B38513 2002.

Bauer:2002:PPB

[Bau02b] Mick Bauer. Paranoid penguin: BestCrypt: Cross-platform filesystem encryption. *Linux Journal*, 98: ??, June 2002. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://www.linuxjournal.com/article.php?sid=5938.

Bauer:2003:PPAa

[Bau03a] Mick Bauer. Paranoid penguin: Authenticate with LDAP. *Linux Journal*, 2003(112):12, August 2003. CODEN LIJOFX. ISSN

1075-3583 (print), 1938-3827 (electronic).

Bauer:2003:PPAb

[Bau03b] Mick Bauer. Paranoid penguin: Authenticate with LDAP, Part III. *Linux Journal*, 2003(113):13, September 2003. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Baudet:2005:DSP

[Bau05] Mathieu Baudet. Deciding security of protocols against off-line guessing attacks. In Meadows and Syverson [MS05b], pages 16–25. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Bauer:2007:DSM

[Bau07] Friedrich Ludwig Bauer. *Decrypted secrets: methods and maxims of cryptology*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., fourth edition, 2007. ISBN 3-540-24502-2. xii + 524 pp. LCCN QA76.9.A25 B38513 2007. URL http://www.loc.gov/catdir/enhancements/fy0824/2006933429-d.html; http://www.loc.gov/catdir/toc/fy0711/2006933429.html.

Bauer:2008:EHE

[Bau08] Friedrich L. Bauer. Erich Hüttenhain: Entzifferung 1939–1945. (German) [Erich Hüttenhain: deciphering 1939–1945]. *Informatik Spektrum*, 31(3):??, ???? 2008. CODEN INSKDW. ISSN 0170-6012 (print), 1432-122X (electronic). URL http://link.springer.com/article/10.1007/s00287-008-0242-4.

Blakley:1979:RSA

[BB79] G. R. Blakley and I. Borosh. Rivest–Shamir–Adleman public key cryptosystems do not always conceal messages. *Computers and Mathematics with Applications*, 5(3):169–178, 1979. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Benedens:2000:TBD

[BB00a] Oliver Benedens and Christoph Busch. Towards blind detection of robust watermarks in polygonal models. *Computer Graphics Forum*, 19(3):??, August 2000. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic). URL aid=412& http://www.blackwellpublishers.co.uk/asp/journal.asp?ref=0167-7055& iid=3& src=ard& vid=19.

Buchmann:2000:ECC

[BB00b] Johannes Buchmann and Harald Baier. Efficient construction of cryptographically strong elliptic curves. *Lecture Notes in Computer Science*, 1977: 191–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1977/19770191.htm; http://link.springer-ny.com/link/service/series/0558/papers/1977/19770191.pdf.

Barkan:2002:HMW

[BB02] Elad Barkan and Eli Biham. In how many ways can you write rijndael? *Lecture Notes in Computer Science*, 2501:160–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010160.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010160.pdf.

Bouda:2003:EQI

[BB03] Jan Bouda and Vladimír R. Bužek. Encryption of quantum information. *International Journal of Foundations of Computer Science (IJFCS)*, 14(5):741–??, October 2003. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Boneh:2004:SIB

[BB04] Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Franklin [Fra04], pages 443–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Bicakci:2005:ISA

[BB05] Kemal Bicakci and Nazife Baykal. Improved server assisted signatures. *Computer Networks (Amsterdam, Netherlands: 1999)*, 47(3):351–366, February 21, 2005. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Biham:2002:SQK

[BBB+02] Eli Biham, Michel Boyer, Gilles Brassard, Jeroen van de Graaf, and Tal Mor. Security of quantum key distribution against all collective attacks. *Algorithmica*, 34(4):372–388, November 2002. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://www.springerlink.com/

openurl.asp?genre=article&issn=0178-4617&volume=34&issue=4&spage=372. Quantum computation and quantum cryptography.

Basso:2009:NBB

[BBC+09] Alessandro Basso, Francesco Bergadano, Davide Cavagnino, Victor Pomponiu, and Annamaria Vernone. A novel block-based watermarking scheme using the SVD transform. *Algorithms (Basel)*, 2(1):46–75, March 2009. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL https://www.mdpi.com/1999-4893/2/1/46.

Behrmann:2002:UIS

[BBD+02] Gerd Behrmann, Johan Bengtsson, Alexandre David, Kim G. Larsen, Paul Pettersson, and Wang Yi. UPPAAL implementation secrets. *Lecture Notes in Computer Science*, 2469: 3–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2469/24690003.htm; http://link.springer.de/link/service/series/0558/papers/2469/24690003.pdf.

Bernstein:2009:PQC

[BBD09] Daniel J. (Daniel Julius) Bernstein, Johannes Buchmann, and Erik Dahmén, editors. *Post-quantum cryptography: [First International Workshop on Post-Quantum Cryptography ... at the Katholieke Universiteit Leuven in 2006]*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Beimel:2000:CFS

[BBDK00] Amos Beimel, Mike Burmester, Yvo Desmedt, and Eyal Kushilevitz. Computing functions of a shared secret. *SIAM Journal on Discrete Mathematics*, 13(3): 324–345, 2000. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/28881.

Bellare:2001:KPP

[BBDP01] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. *Lecture Notes in Computer Science*, 2248: 566–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480566.htm; http://link.springer-

ny.com/link/service/series/0558/papers/2248/22480566.pdf.

Blumenthal:2002:SAD

[BBG+02] Uri Blumenthal, Milind M. Buddhikot, Juan A. Garay, Scott C. Miller, Sarvar Patel, Luca Salgarelli, and Dorothy Stanley. A scheme for authentication and dynamic key exchange in wireless networks. *Bell Labs Technical Journal*, 7(2):37–48, Summer 2002. CODEN BLTJFD. ISSN 1089-7089 (print), 1538-7305 (electronic).

Bartolini:2008:EIS

[BBGM08] S. Bartolini, I. Branovic, R. Giorgi, and E. Martinelli. Effects of instruction-set extensions on an embedded processor: a case study on elliptic curve cryptography over $GF(2^m)$. *IEEE Transactions on Computers*, 57(5):672–685, May 2008. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4358294.

Barkan:2003:ICO

[BBK03a] Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. In Boneh [Bon03], pages 600–616. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Bertoni:2003:EAD

[BBK+03b] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri. Error analysis and detection procedures for a hardware implementation of the advanced encryption standard. *IEEE Transactions on Computers*, 52(4):492–505, April 2003. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1190590.

Bellare:2001:OCH

[BBKN01] Mihir Bellare, Alexandra Boldyreva, Lars Knudsen, and Chanathip Namprempre. Online ciphers and the hash-CBC construction. In Kilian [Kil01a], pages 292–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139.

UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390292.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390292.pdf.

Bellare:2000:PKE

[BBM00] Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. *Lecture Notes in Computer Science*, 1807:259–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070259.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070259.pdf.

Bellare:2009:HPK

[BBN+09] Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. Hedged public-key encryption: How to protect against bad randomness. In ????, editor, *Advances in Cryptology – ASIACRYPT 2009*, pages 232–249. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN ???? LCCN ???? URL ????.

Bobineau:2000:PSD

[BBPV00] Christophe Bobineau, Luc Bouganim, Philippe Pucheral, and Patrick Valduriez. PicoDMBS: Scaling down database techniques for the Smartcard. In El Abbadi et al. [EBC+00], pages 11–20. ISBN 1-55860-715-3. LCCN ???? URL http://www.vldb.org/dblp/db/conf/vldb/ChristopheBPV00.html.

Boneh:2004:SGS

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Franklin [Fra04], pages 41–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Burgess:2001:ISC

[BC01] N. Burgess and L. Ciminiera, editors. *15th IEEE Symposium on Computer Arithmetic: ARITH-15 2001: proceedings: Vail, Colorado, 11–13 June, 2001*. IEEE Computer Society Press, 1109 Spring

Street, Suite 300, Silver Spring, MD 20910, USA, 2001. ISBN 0-7695-1150-3; 0-7695-1152-X. ISSN 1063-6889. LCCN QA76.9.C62 S95 2001. US$145. IEEE order no. PR01150.

Biham:2004:NCS

[BC04a] Eli Biham and Rafi Chen. Near-collisions of SHA-0. In Franklin [Fra04], pages 290–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Blundo:2004:SIA

[BC04b] Carlo Blundo and Stelvio Cimato. A software infrastructure for authenticated Web metering. *Computer*, 37(4):28–??, April 2004. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/comp/mags/co/2004/04/r4028abs.htm; http://csdl.computer.org/dl/mags/co/2004/04/r4028.htm; http://csdl.computer.org/dl/mags/co/2004/04/r4028.pdf.

Backes:2005:PKS

[BC05a] Michael Backes and Christian Cachin. Public-key steganography with active attacks. In Kilian [Kil05], pages 210–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Bergadano:2005:DPL

[BC05b] Francesco Bergadano and Davide Cavagnino. Dealing with packet loss in the interactive chained stream authentication protocol. *Computers & Security*, 24(2):139–146, March 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001877.

Blundo:2005:SCN

[BC05c] Carlo Blundo and Stelvio Cimato, editors. *Security in communication networks: 4th international conference, SCN 2004, Amalfi, Italy, September 8–10, 2004: Revised selected papers*, volume 3352 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-24301-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK5105.59 .S385 2004. URL http://springerlink.metapress.com/openurl.asp?genre=issue&issn=0302-9743&volume=3352; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3352; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b105083.

Brzezinski:2005:MRL

[BCB+05] Zbigniew Brzeziński, Jan Stanisław Ciechanowski, Antoni Bohdanowicz, Witold Zbirohowski-Kościa, et al. *Marjan Rejewski 1905–1980: living with the Enigma secret*. Wydawnictwo Tekst Sp. z o.o., Bydgoszcz, Poland, 2005. ISBN 83-7208-117-4. 288 pp. LCCN ???? Introduction by Professor Zbigniew Brzeziński.

Bergadano:2001:CSA

[BCC01] Francesco Bergadano, Davide Cavagnino, and Bruno Crispo. Chained stream authentication. *Lecture Notes in Computer Science*, 2012:144–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120144.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120144.pdf.

Bergadano:2002:IAM

[BCC02] F. Bergadano, D. Cavagnino, and B. Crispo. Individual authentication in multiparty communications. *Computers & Security*, 21(8):719–735, November 2002. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404802008131.

Brier:2001:CRS

[BCCN01] Eric Brier, Christophe Clavier, Jean-Sébastien Coron, and David Naccache. Cryptanalysis of RSA signatures with fixed-pattern padding. In Kilian [Kil01a], pages 433–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390433.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390433.pdf.

Blundo:2006:VCS

[BCD06] Carlo Blundo, Stelvio Cimato, and Alfredo De Santis. Visual cryptography schemes with optimal pixel expansion. *Theoretical Computer Science*, 369(1–3):169–182, December 15, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Bruguera:2009:PIS

[BCDH09] Javier D. Bruguera, Marius Cornea, Debjit DasSarma, and John Harrison, editors. *Proceedings of the 19th IEEE Symposium on Computer Arithmetic, June 8–10, 2009, Portland, Oregon, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. ISBN 0-7695-3670-0, 1-4244-4329-6. ISSN 1063-6889. LCCN QA76.6 .S887 2009. URL http://www.ac.usc.es/arith19/.

Burnett:2000:EMG

[BCDM00] L. Burnett, G. Carter, E. Dawson, and W. Millan. Efficient methods for generating MARS-like S-boxes (abstract only). In NIST [NIS00], page 10. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Barnum:2002:AQM

[BCG+02] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In IEEE [IEE02], pages 449–458. CODEN ASFPDV. ISBN 0-7695-1822-2. ISSN 0272-5428. LCCN QA267. URL http://ieeexplore.ieee.org/iel5/8411/26517/01181969.pdf?isnumber=26517&prod=CNF&arnumber=1181969&arSt=+449&ared=+458&arAuthor=Barnum%2C+H.%3B+Crepeau%2C+C.%3B+Gottesman%2C+D.%3B+Smith%2C+A.%3B+Tapp%2C+A.; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=26517&arnumber=1181969&count=82&index=45. IEEE Computer Society Order Number PR01822.

Bahi:2011:ECS

[BCGH11] Jacques M. Bahi, Raphaël Couturier, Christophe Guyeux, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of chaotic pseudorandom numbers on GPU. *arxiv.org*, ?? (??):??, December 22, 2011. URL http://arxiv.org/abs/1112.5239.

Brown:2000:PCW

[BCH+00] Michael Brown, Donny Cheung, Darrel Hankerson, Julio Lopez Hernandez, Michael Kirkup, and Alfred Menezes. PGP in constrained wireless devices. In USENIX [USE00d], page ?? ISBN 1-880446-18-9. LCCN ???? URL http://www.usenix.org/publications/library/proceedings/sec2000/brown.html.

Breunesse:2005:FMS

[BCHJ05] C.-B. Breunesse, N. Cataño, M. Huisman, and B. Jacobs. Formal methods for smart cards: an experience report. *Science of Computer Programming*, 55(1–3):53–80, March 2005. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic).

Boneh:2007:CCS

[BCHK07] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *SIAM Journal on Computing*, 36(5):1301–1328, ???? 2007. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Butler:2006:FAK

[BCJ+06] Frederick Butler, Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov, and Christopher Walstad. Formal analysis of Kerberos 5. *Theoretical Computer Science*, 367(1–2):57–87, November 24, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Barni:2005:DWI

[BCKK05] Mauro Barni, Ingemar Cox, Ton Kalker, and Hyoung Joong Kim, editors. *Digital watermarking: 4th international workshop, IWDW 2005, Siena, Italy, September 15–17, 2005: proceedings*, volume 3710 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-28768-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ????

Bao:2005:PSS

[BCL05a] Haiyong Bao, Zhenfu Cao, and Rongxing Lu. Proxy signature scheme using self-certified public keys. *Applied Mathematics and Computation*, 169(2):1380–1389, October 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Barak:2005:SCA

[BCL+05b] Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. In Shoup [Sho05a], pages 361–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Bresson:2001:PAG

[BCP01] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably authenticated group Diffie–Hellman key exchange — the dynamic case. *Lecture Notes in Computer Science*, 2248: 290–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480290.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480290.pdf.

Bresson:2002:DGD

[BCP02a] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Dynamic group Diffie–Hellman key exchange under standard assumptions. *Lecture Notes in Computer Science*, 2332:321–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320321.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320321.pdf.

Bresson:2002:GDH

[BCP02b] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Group Diffie–Hellman key exchange secure against dictionary attacks. *Lecture Notes in Computer Science*, 2501:497–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010497.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010497.pdf.

Bolle:2003:GB

[BCP+03] Ruud Bolle, Jonathan Connell, Sharatchandra Pankanti, Nalini Ratha, and Andrew Senior. *Guide to biometrics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 0-387-40089-3. 335 (est.)

pp. LCCN TK7882.B56 G85 2003. US$49.95.

Bresson:2007:PSA

[BCP07] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably secure authenticated group Diffie–Hellman key exchange. *ACM Transactions on Information and System Security*, 10(3):10:1–10:??, July 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bellavista:2002:JLD

[BCS02] Paolo Bellavista, Antonio Corradi, and Cesare Stefanelli. Java for on-line distributed monitoring of heterogeneous systems and services. *The Computer Journal*, 45(6):595–607, ???? 2002. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_06/450595.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_06/pdf/450595.pdf.

Biham:2008:BA

[BCS08] E. Biham, Y. Carmeli, and A. Shamir. Bug attacks. In ????, editor, *Advances in Cryptology, Proceedings of CRYPTO 08*, volume 5157, pages 221–240. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008.

Betarte:2000:SSC

[BCST00] Gustavo Betarte, Cristina Cornes, Nora Szasz, and Alvaro Tasistro. Specification of a smart card operating system. *Lecture Notes in Computer Science*, 1956:77–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1956/19560077.htm; http://link.springer-ny.com/link/service/series/0558/papers/1956/19560077.pdf.

Bao:2005:RWH

[BCW05] Haiyong Bao, Zhenfu Cao, and Shengbao Wang. Remarks on Wu–Hsu's threshold signature scheme using self-certified public keys. *The Journal of Systems and Software*, 78(1):56–59, October 2005. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Biham:2000:CAG

[BD00a] Eli Biham and Orr Dunkelman. Cryptanalysis of the A5/1 GSM stream cipher. *Lecture Notes in Computer Science*, 1977:43–51, 2000. CODEN LNCSD9. ISSN

0302-9743 (print), 1611-3349 (electronic).

Boneh:2000:CRP

[BD00b] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Transactions on Information Theory*, 46 (4):1339–1349, April 2000. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Bourbakis:2003:SBC

[BD03] Nikolaos Bourbakis and Apostolos Dollas. SCAN-based compression-encryption-hiding for video on demand. *IEEE MultiMedia*, 10(3):79–87, July–September 2003. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://csdl.computer.org/comp/mags/mu/2003/03/u3079abs.htm; http://csdl.computer.org/dl/mags/mu/2003/03/u3079.htm; http://csdl.computer.org/dl/mags/mu/2003/03/u3079.pdf.

Bozzano:2004:AVS

[BD04a] Marco Bozzano and Giorgio Delzanno. Automatic verification of secrecy properties for linear logic specifications of cryptographic protocols. *Journal of Symbolic Computation*, 38(5):1375–1415, November 2004. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Burmester:2004:HPK

[BD04b] Mike Burmester and Yvo G. Desmedt. Is hierarchical public-key certification the next target for hackers? *Communications of the Association for Computing Machinery*, 47(8):68–74, August 2004. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Buchmann:2008:PQC

[BD08] Johannes Buchmann and Jintai Ding, editors. *Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17–19, 2008 Proceedings*, volume 5299 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 3-540-88402-5 (paperback), 3-540-88403-3 (pdf), 3-540-88701-6. LCCN QA76.9.A25 P63 2008. URL http://www.springer.com/computer/security+and+cryptology/book/978-3-540-88402-6.

Biryukov:2003:CS

[BDD03] Alex Biryukov, Christophe De Cannière, and Gustaf Dellkrantz. Cryptanalysis of Safer++. In Boneh [Bon03], pages 195–211. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Blundo:2003:COT

[BDDS03] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson. Contrast optimal threshold visual cryptography schemes. *SIAM Journal on Discrete Mathematics*, 16 (2):224–261, 2003. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/33668.

Bolosky:2000:FSD

[BDET00] William J. Bolosky, John R. Douceur, David Ely, and Marvin Theimer. Feasibility of a serverless distributed file system deployed on an existing set of desktop PCs. *ACM SIGMETRICS Performance Evaluation Review*, 28(1): 34–43, June 2000. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Bao:2001:SPD

[BDF+01a] Feng Bao, Robert Deng, Peirong Feng, Yan Guo, and Hongjun Wu. Secure and private distribution of online video and some related cryptographic issues. *Lecture Notes in Computer Science*, 2119:190–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190190.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190190.pdf.

Boneh:2001:LBM

[BDF01b] Dan Boneh, Glenn Durfee, and Matt Franklin. Lower bounds for multicast message authentication. *Lecture Notes in Computer Science*, 2045:437–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450437.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450437.pdf.

Bodei:2002:PAP

[BDFP02] Chiara Bodei, Pierpaolo

Degano, Riccardo Focardi, and Corrado Priami. Primitives for authentication in process algebras. *Theoretical Computer Science*, 283(2):271–304, June 2002. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Bodei:2005:APS

[BDFP05] C. Bodei, P. Degano, R. Focardi, and C. Priami. Authentication primitives for secure protocol specifications. *Future Generation Computer Systems*, 21(5): 645–653, May 2005. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Bao:2001:CTS

[BDG+01] Feng Bao, Robert H. Deng, Willi Geiselmann, Claus Schnorr, Rainer Steinwandt, and Hongjun Wu. Cryptanalysis of two sparse polynomial based public key cryptosystems. *Lecture Notes in Computer Science*, 1992:153–164, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920153.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920153.pdf.

Bhattacharyya:2009:VPA

[BDhKB09] D. Bhattacharyya, P. Das, T. h. Kim, and S. K. Bandyopadhyay. Vascular pattern analysis towards pervasive palm vein authentication. *J.UCS: Journal of Universal Computer Science*, 15 (5):1081–??, ???? 2009. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_15_5/vascular_pattern_analysis_towards.

Biham:2002:EDL

[BDK02a] Eli Biham, Orr Dunkelman, and Nathan Keller. Enhancing differential-linear cryptanalysis. *Lecture Notes in Computer Science*, 2501: 254–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010254.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010254.pdf.

Biham:2002:LCR

[BDK02b] Eli Biham, Orr Dunkelman, and Nathan Keller. Linear cryptanalysis of reduced round serpent. *Lecture Notes in Computer Science*, 2355:16–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/

bibs/2355/23550016.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550016.pdf.

Biryukov:2009:KRA

[BDK+09] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES variants with up to 10 rounds. Report, University of Luxembourg, Luxembourg; École Normale Supérieure, 45 rue d'Ulm, 75230 Paris, France. Einstein Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel; Computer Science department, The Weizmann Institute, Rehovot 76100, Israel, November 8, 2009. URL http://eprint.iacr.org/2009/374.pdf.

Blundo:2000:VCG

[BDN00] Carlo Blundo, Alfredo De Santis, and Moni Naor. Visual cryptography for grey level images. *Information Processing Letters*, 75 (6):255–259, November 30, 2000. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.nl/gej-ng/10/23/20/64/31/27/abstract.html; http://www.elsevier.nl/gej-ng/10/23/20/64/31/27/article.pdf.

Bodei:2002:FLD

[BDNN02] C. Bodei, P. Degano, F. Nielson, and H. Riis Nielson. Flow logic for Dolev–Yao secrecy in cryptographic processes. *Future Generation Computer Systems*, 18(6):747–756, May 2002. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Boreale:2002:PTC

[BDP02] Michele Boreale, Rocco De Nicola, and Rosario Pugliese. Proof techniques for cryptographic processes. *SIAM Journal on Computing*, 31(3):947–986, June 2002. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/37786.

Bertoni:2009:RPK

[BDPV09] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The road from Panama to Keccak via RadioGatún. In Helena Handschuh, Stefan Lucks, Bart Preneel, and Phillip Rogaway, editors, *Symmetric Cryptography*, number 09031 in Dagstuhl Seminar Proceedings, page ?? Schloss Dagstuhl — Leibniz-Zentrum für Informatik, Germany, Dagstuhl, Germany, 2009. ISSN 1862-4405. URL http://drops.dagstuhl.de/opus/volltexte/2009/1958.

Biryukov:2004:MLA

[BDQ04] Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On multiple linear approximations. In Franklin [Fra04], pages 1–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Baldwin:2009:PSS

[BDS+09a] Adrian Baldwin, Chris Dalton, Simon Shiu, Krzysztof Kostienko, and Qasim Rajpoot. Providing secure services for a virtual infrastructure. *Operating Systems Review*, 43(1):44–51, January 2009. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Buchmann:2009:HBD

[BDS09b] Johannes Buchmann, Erik Dahmen, and Michael Szydlo. Hash-based digital signature schemes. In Bernstein et al. [BBD09], pages 35–94. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Bertolotti:2008:ERA

[BDSV08] Ivan Cibrario Bertolotti, Luca Durante, Riccardo Sisto, and Adriano Valenzano. Efficient representation of the attacker's knowledge in cryptographic protocols analysis. *Formal Aspects of Computing*, 20(3):303–348, May 2008. CODEN FACME5. ISSN 0934-5043 (print), 1433-299X (electronic). URL http://link.springer.com/article/10.1007/s00165-008-0078-3.

Boneh:2001:MFR

[BDTW01] Dan Boneh, Xuhua Ding, Gene Tsudik, and Chi Ming Wong. A method for fast revocation of public key certificates and security capabilities. In USENIX [USE01c], page ?? ISBN 1-880446-18-9, 1-880446-07-3. LCCN QA76.9.A25 U565 2001. URL http://www.usenix.org/publications/library/proceedings/sec01/boneh.html.

Bao:2004:PKC

[BDZ04] Feng Bao, Robert Deng, and Jianying Zhou, editors. *Public Key Cryptography—PKC 2004: 7th International Workshop on Practice and Theory in Pub-*

lic Key Cryptography, Singapore, March 1–4, 2004: Proceedings, volume 2947 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-21018-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I567 2004. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2947.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2947; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b95631.

Beckman:2002:CAB

[Bec02] Bengt Beckman. *Codebreakers: Arne Beurling and the Swedish crypto program during World War II*. American Mathematical Society, Providence, RI, USA, 2002. ISBN 0-8218-2889-4. xviii + 259 pp. LCCN D810.C88 B413 2002.

Beebe:2005:CBPd

[Bee05] Nelson H. F. Beebe. A complete bibliography of publications in *Designs, Codes, and Cryptography*. Technical report, University of Utah, Department of Mathematics, Salt Lake City, UT 84112-0090, USA, July 6, 2005. 107 pp. URL https://www.math.utah.edu/pub/tex/bib/index-table-d.html#designscodescryptogr.

Bejtlich:2006:EDS

[Bej06] Richard Bejtlich. *Extrusion detection: security monitoring for internal intrusions*. Addison-Wesley, Reading, MA, USA, 2006. ISBN 0-321-34996-2 (paperback). xxviii + 385 pp. LCCN TK5105.59 .B43 2006.

Bellare:2000:ACC

[Bel00] Mihir Bellare, editor. *Advances in cryptology — CRYPTO 2000: 20th annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 2000: proceedings*, volume 1880 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar.

Bella:2001:MPS

[Bel01] Giampaolo Bella. Mechanising a protocol for smart cards. *Lecture Notes in Computer Science*, 2140: 19–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400019.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400019.pdf.

Bellovin:2004:IRS

[Bel04] Steven M. Bellovin. Inside risks: Spamming, phishing, authentication, and privacy. *Communications of the Association for Computing Machinery*, 47(12):144, December 2004. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Belfield:2007:SUC

[Bel07a] Richard Belfield. *The six unsolved ciphers: inside the mysterious codes that have confounded the world's greatest cryptographers*. Ulysses, Berkeley, CA, USA, 2007. ISBN 1-56975-628-7 (paperback). ix + 281 + 16 pp. LCCN Z103 .B45 2007.

Bella:2007:FCS

[Bel07b] Giampaolo Bella. *Formal correctness of security protocols*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-68134-5, 3-540-68136-1 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xviii + 274 + 62 pp. LCCN QA8.9-QA10.3; TK5105.59.B45 2007.

Bello:2008:OPR

[Bel08] L. Bello. `openssl` — predictable random number generator. Debian security advisory 1571-1., 2008.

Bruss:2007:QCS

[BEM+07] Dagmar Bruss, Gábor Erdélyi, Tim Meyer, Tobias Riege, and Jörg Rothe. Quantum cryptography: a survey. *ACM Computing Surveys*, 39(2):1–27, ???? 2007. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Benedens:2000:AIW

[Ben00] Oliver Benedens. Affine invariant watermarks for 3D polygonal and NURBS based models. *Lecture Notes in Computer Science*, 1975:15–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750015.htm; http://link.springer-ny.com/link/service/series/0558/papers/1975/19750015.pdf.

Benantar:2001:IPK

[Ben01a] M. Benantar. The Internet public key infrastructure. *IBM Systems Journal*, 40(3):648–665, ???? 2001. CODEN IBMSA7. ISSN 0018-8670. URL http://www.research.ibm.com/journal/sj/403/benantar.html; http://www.research.ibm.com/journal/sj/403/benantar.pdf.

Benson:2001:VS

[Ben01b] Robert L. Benson. The Venona story. Report ????, Center for Cryptologic History, National Security Agency, Fort Meade, MD, USA, ???? 2001.

Benantar:2002:IPK

[Ben02] Messaoud Benantar. *Introduction to the Public Key Infrastructure for the Internet*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 2002. ISBN 0-13-060927-7. xii + 254 pp. LCCN QA76.9.A25 B45 2002. US$54.99. URL http://www.phptr.com/ptrbooks/ptr_0130609277.html.

Benson:2004:VS

[Ben04] Robert L. Benson. The Venona story. Report, Center for Cryptologic History, National Security Agency, 9800 Savage Road, Suite 6886, Fort George G. Meade, MD 20755-6886, January 15, 2004. 63 pp. URL https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/assets/files/venona_story.pdf.

Berson:2000:CE

[Ber00] Thomas A. Berson. Cryptography everywhere. *Lecture Notes in Computer Science*, 1976:72–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760072.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760072.pdf.

Berson:2003:CAB

[Ber03] Tom Berson. Cryptography after the bubble: How to make an impact on the world. In Joye [Joy03b], page 226. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Bernstein:2004:FPA

[Ber04] Daniel J. Bernstein. Floating-point arithmetic and message authentication, September 18, 2004. URL `https://cr.yp.to/antiforgery/hash127-20040918.pdf`. To be incorporated into the author's *High-Speed Cryptography* book. [As of 13 May 2024, this book seems not to have been published.].

Bernstein:2007:SFS

[Ber07] Daniel J. Bernstein. The Salsa20 family of stream ciphers. Report, Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, Chicago, IL 60607-7045, December 25, 2007. URL `http://cr.yp.to/snuffle/salsafamily-20071225.pdf`.

Bernstein:2008:CVS

[Ber08] Daniel J. Bernstein. ChaCha, a variant of Salsa20. Report, Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, Chicago, IL 60607-7045, January 28, 2008. URL `http://cr.yp.to/chacha/chacha-20080128.pdf`.

Bergmann:2009:DKR

[Ber09a] Seth D. Bergmann. Degenerate keys for RSA encryption. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 41(2):95–98, June 2009. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Bernstein:2009:IPQ

[Ber09b] Daniel J. Bernstein. Introduction to post-quantum cryptography. In Bernstein et al. [BBD09], pages 1–14. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Bouwmeester:2000:PQI

[BEZ00] Dirk Bouwmeester, Artur K. Ekert, and Anton Zeilinger. *The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-66778-4. xvi + 314 pp. LCCN QA76.889 .P47 2000.

Bouwmeester:2001:PQI

[BEZ01] Dirk Bouwmeester, Artur Ekert, and Anton Zeilinger, editors. *The physics of quantum information: Quantum cryptography, quantum teleportation, quantum computation*. Physics and astronomy online library. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-

540-66778-4. xvi + 314 pp. LCCN QA76.889 .P47 2000.

Biham:2000:IDR

[BF00a] Eli Biham and Vladimir Furman. Impossible differential on 8-round MARS' core. In NIST [NIS00], pages 186–194. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Biham:2000:IID

[BF00b] Eli Biham and Vladimir Furman. Improved impossible differentials on Twofish. *Lecture Notes in Computer Science*, 1977: 80–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1977/19770080.htm; http://link.springer-ny.com/link/service/series/0558/papers/1977/19770080.pdf.

Babbage:2001:MHO

[BF01a] Steve Babbage and Laurent Frisch. On MISTY1 higher order differential cryptanalysis. *Lecture Notes in Computer Science*, 2015:22–36, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boneh:2001:IBE

[BF01b] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In Kilian [Kil01a], pages 213–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390213.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390213.pdf.

Boneh:2001:EGS

[BF01c] Dan Boneh and Matthew Franklin. Efficient generation of shared RSA keys. *Journal of the ACM*, 48(4): 702–722, July 2001. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Boneh:2003:IBE

[BF03] Dan Boneh and Matthew Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, June 2003. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/39852`.

Boldyreva:2005:ARO

[BF05] Alexandra Boldyreva and Marc Fischlin. Analysis of random oracle instantiation scenarios for OAEP and other practical schemes. In Shoup [Sho05a], pages 412–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621`.

Bisseling:2006:MSM

[BF06a] Rob H. Bisseling and Ildikó Flesch. Mondriaan sparse matrix partitioning for attacking cryptosystems by a parallel block Lanczos algorithm — a case study. *Parallel Computing*, 32(7–8):551–567, September 2006. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Boldyreva:2006:SO

[BF06b] Alexandra Boldyreva and Marc Fischlin. On the security of OAEP. *Lecture Notes in Computer Science*, 4284:210–225, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11935230_14.pdf`.

Bhargavan:2008:CVI

[BFCZ08] Karthikeyan Bhargavan, Cédric Fournet, Ricardo Corin, and Eugen Zalinescu. Cryptographically verified implementations for `tls`. In ????, editor, *ACM Conference on Computer and Communications Security*, pages 459–468. ACM Press, New York, NY 10036, USA, 2008. ISBN ???? LCCN ???? URL `????`.

Bhargavan:2004:SWS

[BFG04] Karthikeyan Bhargavan, Cédric Fournet, and Andrew D. Gordon. A semantics for Web services authentication. *ACM SIGPLAN Notices*, 39(1):198–209, January 2004. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Bhargavan:2005:SWS

[BFG05] Karthikeyan Bhargavan, Cédric Fournet, and Andrew D. Gordon. A semantics for web services authentication. *Theoretical Computer Science*, 340(1):102–153, June 13, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Bhargavan:2008:VPB

[BFG08] Karthikeyan Bhargavan, Cédric Fournet, and Andrew D. Gordon. Verifying policy-based web services security. *ACM Transactions on Programming Languages and Systems*, 30(6): 30:1–30:59, October 2008. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).

Bhargavan:2008:VII

[BFGT08] Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon, and Stephen Tse. Verified interoperable implementations of security protocols. *ACM Transactions on Programming Languages and Systems*, 31(1):5:1–5:57, December 2008. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).

Bugliesi:2007:DTA

[BFM07] Michele Bugliesi, Riccardo Focardi, and Matteo Maffei. Dynamic types for authentication. *Journal of Computer Security*, 15 (6):563–617, ???? 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Biham:2002:DCQ

[BFMR02] Eli Biham, Vladimir Furman, Michal Misztal, and Vincent Rijmen. Differential cryptanalysis of Q. *Lecture Notes in Computer Science*, 2355:174–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550174.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550174.pdf`.

Brown:2007:SAN

[BG07a] Daniel R. L. Brown and Kristian Gjøsteen. A security analysis of the NIST SP 800-90 elliptic curve random number generator. In Menezes [Men07], pages 466–481. ISBN 3-540-74142-9 (paperback). LCCN QA76.9.A25 C79 2007. URL `http://dl.acm.org/citation.cfm?id=1777777.1777815`.

Bugliesi:2007:SIT

[BG07b] Michele Bugliesi and Marco Giunti. Secure implementations of typed channel abstractions. *ACM SIGPLAN Notices*, 42(1):251–262, January 2007. CODEN

SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Blaszczyk:2008:NMT

[BG08] M. Blaszczyk and R. A. Guinee. A novel modelled true random binary number generator for key stream generation in cryptographic applications. In *MILCOM 2008. IEEE Military Communications Conference, 2008*, pages 1–7. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4753211`.

Blaszczyk:2009:EVT

[BG09] Marta Blaszczyk and Richard A. Guinee. Experimental validation of a true random binary digit generator fusion with a pseudo random number generator for cryptographic module application. In *IET Irish Signals and Systems Conference (ISSC 2009)*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5524689`.

Barthe:2009:FCC

[BGB09] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. Formal certification of code-based cryptographic proofs. *ACM SIGPLAN Notices*, 44(1):90–101, January 2009. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Boneh:2007:SEI

[BGH07] D. Boneh, C. Gentry, and M. Hamburg. Space-efficient identity based encryption without pairings. In IEEE [IEE07], pages 647–657. ISBN 0-7695-3010-9. ISSN 0272-5428. LCCN QA76 .S974 2007. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=4389466`. IEEE Computer Society order number P3010.

Bennett:2002:ESE

[BGHP02] Krista Bennett, Christian Grothoff, Tzvetan Horozov, and Ioana Patrascu. Efficient sharing of encrypted data. *Lecture Notes in Computer Science*, 2384: 107–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840107.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2384/23840107.pdf`.

Barak:2001:IPO

[BGI+01] Boaz Barak, Oded Goldreich, Rusell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In Kilian [Kil01a], pages 1–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390001.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390001.pdf.

Bogomjakov:2008:PMD

[BGI08] Alexander Bogomjakov, Craig Gotsman, and Martin Isenburg. Points and meshes: Distortion-free steganography for polygonal meshes. *Computer Graphics Forum*, 27(2):637–642, April 2008. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Bertoni:2003:EAA

[BGK+03] Guido Bertoni, Jorge Guajardo, Sandeep Kumar, Gerardo Orlando, Christof Paar, and Thomas Wollinger. Efficient $GF(p^m)$ arithmetic architectures for cryptographic applications. In Joye [Joy03b], pages 158–175. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Bucci:2003:HSO

[BGL+03] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC. *IEEE Transactions on Computers*, 52(4):403–409, April 2003. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1190581.

Boneh:2003:AVE

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. *Lecture Notes in Computer Science*, 2656: 416–432, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_26.pdf.

Branovic:2004:WCE

[BGM04] I. Branovic, R. Giorgi, and E. Martinelli. A workload characterization of elliptic curve cryptography methods in embedded environments. *ACM SIGARCH Computer Architecture News*, 32(3):27–34, June 2004. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Boyer:2009:SBB

[BGM09] Michel Boyer, Ran Gelles, and Tal Mor. Security of the Bennett–Brassard quantum key distribution protocol against collective attacks. *Algorithms (Basel)*, 2(2):790–807, June 2009. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL https://www.mdpi.com/1999-4893/2/2/790.

Boneh:2005:EDF

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In Kilian [Kil05], pages 325–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Boldyreva:2008:NMS

[BGOY08] Alexandra Boldyreva, Craig Gentry, Adam O'Neill, and Dae Hyun Yum. New multiparty signature schemes for network routing applications. *ACM Transactions on Information and System Security*, 12(1):3:1–3:??, October 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bergadano:2002:UAT

[BGP02] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security*, 5(4):367–397, November 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Berbain:2009:QMS

[BGP09] Côme Berbain, Henri Gilbert, and Jacques Patarin. QUAD: a multivariate stream cipher with provable security. *Journal of Symbolic Computation*, 44(12):1703–1723, December 2009. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Blackburn:2005:PNP

[BGPGS05] Simon R. Blackburn, Domingo Gomez-Perez, Jaime Gutierrez, and Igor E. Shparlinski. Predicting nonlinear pseudorandom number generators. *Mathematics of Computation*, 74(251):1471–1494, July 2005. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/home.html; http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/S0025-5718-04-01698-9.dvi; http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/S0025-5718-04-01698-9.pdf; http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/S0025-5718-04-01698-9.ps; http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/S0025-5718-04-01698-9.tex; http://www.jstor.org/stable/pdfplus/4100190.pdf.

Boneh:2005:CRB

[BGW05] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Shoup [Sho05a], pages 258–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Beck:2000:FSD

[BH00a] Robert Beck and Steve Holstead. FOKSTRAUT and Samba — dealing with authentication and performance issues on a large-scale Samba service. In USENIX [USE00c], page ?? ISBN 1-880446-13-8. LCCN ???? URL http://www.usenix.org/publications/library/proceedings/lisa2000/beck.html.

Bialaski:2000:SLN

[BH00b] Tom Bialaski and Michael Haines. *Solaris and LDAP Naming Services: Deploying LDAP in the Enterprise*. Sun BluePrints Program. Sun Microsystems Press, Palo Alto, CA, USA, 2000. ISBN 0-13-030678-9. xxvii + 372 pp. LCCN QA76.76.O63B518 2001. URL books/ldap.pdf; http://www.sun.com/books/catalog/haines/. Part No. 806-2893-10 October 2000.

Barak:2005:MAP

[BH05] B. Barak and S. Halevi. A model and architecture for pseudo-ransom generation with applications to /dev/random. In Meadows and Syverson [MS05b], pages 203–212. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Badra:2006:KEA

[BH06] Mohamad Badra and Ibrahim Hajjeh. Key-exchange authentication using shared secrets. *Computer*, 39(3):58–66, March 2006. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Backhouse:2003:TOT

[BHM03] James Backhouse, Carol Hsu, and Aidan McDonnell. Technical opinion: Toward public-key infrastructure interoperability. *Communications of the Association for Computing Machinery*, 46(6):98–100, June 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bajard:2004:FRI

[BI04] J.-C. Bajard and L. Imbert. A full RNS implementation of RSA. *IEEE Transactions on Computers*, 53(6):769–774, June 2004. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1288551.

Barkol:2005:SCC

[BI05a] Omer Barkol and Yuval Ishai. Secure computation of constant-depth circuits with applications to database search problems. In Shoup [Sho05a], pages 395–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Beimel:2005:PNS

[BI05b] Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. *SIAM Journal on Discrete Mathematics*, 19(1):258–280, 2005. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/41286.

Bi:2009:MCE

[Bi09] Chengpeng Bi. A Monte Carlo EM algorithm for De Novo Motif discovery in biomolecular sequences. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 6(3):370–386, July 2009. CODEN ITCBCY. ISSN 1545-

5963 (print), 1557-9964 (electronic).

Bidgoli:2003:EIS

[Bid03] Hossein Bidgoli, editor. *Encyclopedia of information systems*. Academic Press, New York, NY, USA, 2003. ISBN 0-12-227240-4. various pp. LCCN QA76.15 .E516 2003. US$1,200.00. Four volumes.

Biggs:2008:CII

[Big08] Norman Biggs. *Codes: An introduction to Information Communication and Cryptography*. Springer undergraduate mathematics series. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 1-84800-273-4 (e-book), 1-84800-272-6 (paperback). x + 273 pp. LCCN QA268 .B496 2008eb.

Biham:2000:CPR

[Bih00] Eli Biham. Cryptanalysis of Patarin's 2-round public key system with S boxes (2R). *Lecture Notes in Computer Science*, 1807: 408–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070408.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070408.pdf.

Biham:2002:HDE

[Bih02] Eli Biham. How to decrypt or even substitute DES-encrypted messages in 2^{28} steps. *Information Processing Letters*, 84(3):117–124, November 15, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Biham:2003:ACE

[Bih03] Eli Biham, editor. *Advances in cryptology — EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003: Proceedings*, volume 2656 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-14039-5 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2656.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2656. Also available via the World Wide Web.

Beimel:2000:RSC

[BIM00] Amos Beimel, Yuval Ishai, and Tal Malkin. Reducing the servers computation in private information retrieval: PIR with preprocessing. In Bellare [Bel00], pages 55–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800055.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800055.pdf`.

Bajard:2003:EMG

[BINP03] J.-C. Bajard, L. Imbert, C. Negre, and T. Plantard. Efficient multiplication in GF(p_k) for elliptic curve cryptography. In Bajard and Schulte [BS03], pages 181–187. ISBN 0-7695-1894-X. ISSN 1063-6889. LCCN ???? URL `http://www.dec.usc.es/arith16/`. IEEE order no. PR01894.

Bajard:2005:AOP

[BIP05] Jean-Claude Bajard, Laurent Imbert, and Thomas Plantard. Arithmetic operations in the polynomial modular number system. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL `http://arith17.polito.it/final/paper-168.pdf`.

Biryukov:2007:FSE

[Bir07] Alex Biryukov, editor. *Fast software encryption: 14th international workshop, FSE 2007, Luxembourg, Luxembourg, March 26–28, 2007, revised selected papers*, volume 4593 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-74617-X (softcover). LCCN QA76.9.A25 F77 2007. URL `http://www.springerlink.com/openurl.asp?genre=book\%26isbn=978-3-540-74617-1`.

Bishop:2003:ICJ

[Bis03a] David Bishop. *Introduction to cryptography with Java applets*. Jones and Bartlett, Boston, MA, USA, 2003. ISBN 0-7637-2207-3. xvi + 370 pp. LCCN QA76.9.A25 B565 2003.

Bishop:2003:CSA

[Bis03b] Matt Bishop. *Computer Security: Art and Science*. Addison-Wesley, Reading, MA, USA, 2003. ISBN 0-201-44099-7 (hardcover). xli + 1084 pp. LCCN QA76.9.A25 B56 2002. US$79.99, CAN$120.99.

Barkol:2008:CPR

[BIW08] Omer Barkol, Yuval Ishai, and Enav Weinreb. Communication in the presence of replication. In ACM [ACM08], pages 661–670. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Boyce:2002:IAM

[BJ02] Joseph G. Boyce and Dan W. Jennings. *Information assurance: managing organizational IT security risks*. Butterworth-Heinemann, Boston, MA, USA, 2002. ISBN 0-7506-7327-3. xxi + 261 pp. LCCN QA76.9.A25 B69 2002. US$44.95.

Blaser:2002:PCC

[BJLS02] Markus Bläser, Andreas Jakoby, Maciej Liskiewicz, and Bodo Siebert. Private computation — k-connected versus 1-connected networks. In Yung [Yun02a], pages 194–209. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Boneh:2000:WTE

[BJN00] Dan Boneh, Antoine Joux, and Phong Q. Nguyen. Why textbook ElGamal and RSA encryption are insecure (extended abstract). In *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, volume 1976 of *Lecture Notes in Comput. Sci.*, pages 30–43. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760030.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760030.pdf.

Bjorn:2005:BHM

[Bjo05] Vance Bjorn. Biometrics hit the mainstream: an analysis of security and privacy implications. In Meadows and Syverson [MS05b], page 407. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Backes:2002:DCS

[BJP02] Michael Backes, Christian Jacobi, and Birgit Pfitzmann. Deriving cryptographically sound implementations using composition and formally verified bisimulation. *Lecture Notes in Computer Science*, 2391:310–??, 2002. CO-

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2391/23910310.htm; http://link.springer-ny.com/link/service/series/0558/papers/2391/23910310.pdf.

Breunesse:2002:SVD

[BJvdB02] Cees-Bart Breunesse, Bart Jacobs, and Joachim van den Berg. Specifying and verifying a decimal representation in Java for Smart Cards. *Lecture Notes in Computer Science*, 2422: 304–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2422/24220304.htm; http://link.springer-ny.com/link/service/series/0558/papers/2422/24220304.pdf.

Boni:2000:NGT

[BK00] William Boni and Gerald L. Kovacich. *Netspionage: the global threat to information*. Butterworth-Heinemann, Boston, MA, USA, 2000. ISBN 0-7506-7257-9. xx + 260 pp. LCCN HV6773 .B665 2000. US$34.95.

Burnside:2005:CCP

[BK05] Matthew Burnside and Angelos D. Keromytis. The case for crypto protocol awareness inside the OS kernel. *ACM SIGARCH Computer Architecture News*, 33(1):58–64, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Barker:2006:RRN

[BK06a] Elaine Barker and John Kelsey. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2006. viii + 123 pp. URL http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90_DRBG-June2006-final.pdf.

Breveglieri:2006:GEI

[BK06b] L. Breveglieri and I. Koren. Guest Editors' introduction: Special section on fault diagnosis and tolerance in cryptography. *IEEE Transactions on Computers*, 55(9): 1073–1074, September 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1668034.

Barker:2007:RRN

[BK07] Elaine Barker and John Kelsey. *Recommendation* *for random number generation using deterministic random bit generators (revised)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, March 2007. viii + 124 pp. URL http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf.

Barreto:2002:EAP

[BKLS02] Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. In Yung [Yun02a], pages 354–368. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420354.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420354.pdf.

Breveglieri:2007:OCA

[BKM07] L. Breveglieri, I. Koren, and P. Maistri. An operation-centered approach to fault detection in symmetric cryptography ciphers. *IEEE Transactions on Computers*, 56(5):635–649, May 2007. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4118667.

Bellare:2004:BPR

[BKN04] Mihir Bellare, Tadayoshi Kohno, and Chanathip Namprempre. Breaking and provably repairing the SSH authenticated encryption scheme: a case study of the encode-then-encrypt-and-MAC paradigm. *ACM Transactions on Information and System Security*, 7(2):206–241, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bajard:2009:SRB

[BKP09] J. C. Bajard, M. Kaihara, and T. Plantard. Selected RNS bases for modular multiplication. In Bruguera et al. [BCDH09], pages 25–31. ISBN 0-7695-3670-0, 1-4244-4329-6. ISSN 1063-6889. LCCN QA76.6 .S887 2009. URL http://www.ac.usc.es/arith19/.

Bellare:2000:SCB

[BKR00] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences*, 61(3):362–399, December 2000. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002200009991694X.

Blum:2003:NTL

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*, 50(4):506–519, July 2003. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Buonanno:2002:IUE

[BKY02] Enrico Buonanno, Jonathan Katz, and Moti Yung. Incremental unforgeable encryption. *Lecture Notes in Computer Science*, 2355: 109–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550109.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550109.pdf.

Broadfoot:2002:ASA

[BL02] Philippa Broadfoot and Gavin Lowe. Analysing a stream authentication protocol using model checking. *Lecture Notes in Computer Science*, 2502: 146–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2502/25020146.htm; http://link.springer.de/link/service/series/0558/papers/2502/25020146.pdf.

Bucci:2008:FDR

[BL08] M. Bucci and R. Luzzi. Fully digital random bit generators for cryptographic applications. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 55 (3):861–875, ???? 2008. CODEN ???? ISSN 1549-8328 (print), 1558-0806 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4432925.

Black:2000:TDE

[Bla00] Michael Andrew Black. A treatise on data encryption and an example of the black algorithm. Thesis (M.A.), University of California, Santa Barbara, Santa Barbara, CA, USA, 2000.

Blanchet:2001:ACP

[Bla01a] Bruno Blanchet. Abstracting cryptographic protocols by Prolog rules. *Lecture Notes in Computer Science*, 2126:433–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2126/21260433.htm; http://link.springer-ny.com/link/service/series/0558/papers/2126/21260433.pdf.

Blanchet:2001:ECP

[Bla01b] Bruno Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In ????, editor, *IEEE Computer Security Foundations Workshop*, page 82. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2001. ISBN ???? LCCN ???? URL ????.

Blaze:2001:LYS

[Bla01c] Matt Blaze. Loaning your soul to the devil: Influencing policy without selling out, 2001. Unpublished invited talk, Tenth USENIX Security Symposium, August 13–17, 2001, Washington, DC, USA.

Blanchet:2002:SAS

[Bla02a] Bruno Blanchet. From secrecy to authenticity in security protocols. *Lecture Notes in Computer Science*, 2477:342–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2477/24770342.htm; http://link.springer-ny.com/link/service/series/0558/papers/2477/24770342.pdf.

Blaze:2002:CI

[Bla02b] Matt Blaze. Cryptography and insecurity. In USENIX [USE02a], pages viii + 151. ISBN 1-880446-02-2. LCCN QA76.76.O63 B736 2002. URL http://www.usenix.org/publications/library/proceedings/bsdcon02/tech.html. Unpublished invited talk, BSDCON2002: Growing the BSD Community, February 11–14, 2002, Cathedral Hill Hotel, San Francisco, CA.

Blaze:2003:FCI

[Bla03] Matt Blaze, editor. *Financial cryptography: 6th International Conference, FC 2002, Southampton, Bermuda, March 11–14, 2002: Revised Papers*, volume 2357 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-00646-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2357.htm; http:

//www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2357.

Burmester:2009:UCR

[BLDT09] Mike Burmester, Tri Van Le, Breno De Medeiros, and Gene Tsudik. Universally composable RFID identification and authentication protocols. *ACM Transactions on Information and System Security*, 12(4):21:1–21:??, April 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bleumer:2007:EPS

[Ble07] Gerrit Bleumer. *Electronic postage systems: technology, security, economics*, volume 26 of *Advances in information security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 0-387-29313-2 (hardcover). xxiii + 248 pp. LCCN HE6125 .B545 2007. URL http://www.loc.gov/catdir/enhancements/fy0824/2006933129-b.html; http://www.loc.gov/catdir/enhancements/fy0824/2006933129-d.html; http://www.loc.gov/catdir/toc/fy0801/2006933129.html.

Bao:2006:CIB

[BLH06] Feng Bao, Cheng-Chi Lee, and Min-Shiang Hwang. Cryptanalysis and improvement on batch verifying multiple RSA digital signatures. *Applied Mathematics and Computation*, 172(2):1195–1200, January 15, 2006. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Berbecaru:2001:CPK

[BLM01] Diana Berbecaru, Antonio Lioy, and Marius Marian. On the complexity of public-key certificate validation. *Lecture Notes in Computer Science*, 2200:183–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2200/22000183.htm; http://link.springer-ny.com/link/service/series/0558/papers/2200/22000183.pdf.

Brassard:2000:SAP

[BLMS00] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Security aspects of practical quantum cryptography. *Lecture Notes in Computer Science*, 1807:289–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070289.htm;

http://link.springer-ny.com/link/service/series/0558/papers/1807/18070289.pdf.

Bozga:2006:PBA

[BLP06] L. Bozga, Y. Lakhnech, and M. Périn. Pattern-based abstraction for verifying secrecy in protocols. *International Journal on Software Tools for Technology Transfer: STTT*, 8(1):57–76, February 2006. CODEN ???? ISSN 1433-2779 (print), 1433-2787 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1433-2779&volume=8&issue=1&spage=57.

Buchmann:2009:PQC

[BLRS09] Johannes Buchmann, Richard Lindner, Markus Rückert, and Michael Schneider. Post-quantum cryptography: lattice signatures. *Computing*, 85(1–2):105–125, June 2009. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=85&issue=1&spage=105.

Banks:2001:CAS

[BLST01] William D. Banks, Daniel Lieman, Igor E. Shparlinski, and Van Thuong To. Cryptographic applications of sparse polynomials over finite rings. *Lecture Notes in Computer Science*, 2015:206–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2015/20150206.htm; http://link.springer-ny.com/link/service/series/0558/papers/2015/20150206.pdf.

Blunden:2009:RAE

[Blu09] Bill Blunden. *The rootkit arsenal: escape and evasion in the dark corners of the system*. Wordware Publishing, Plano, TX, USA, 2009. ISBN 1-59822-061-6 (paperback). xxvii + 908 pp. LCCN QA76.9.A25 B585 2009.

Batina:2001:AWD

[BM01a] Lejla Batina and Geeke Muurling. Another way of doing RSA cryptography in hardware. *Lecture Notes in Computer Science*, 2260:364–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600364.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600364.pdf.

Blomer:2001:LSE

[BM01b] Johannes Blömer and Alexander May. Low secret exponent RSA revisited. *Lecture Notes in Computer Science*, 2146:4–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2146/21460004.htm; http://link.springer-ny.com/link/service/series/0558/papers/2146/21460004.pdf.

Brincat:2001:KRA

[BM01c] Karl Brincat and Chris J. Mitchell. Key recovery attacks on MACs based on properties of cryptographic APIs. *Lecture Notes in Computer Science*, 2260:63–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600063.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600063.pdf.

Basu:2003:AC

[BM03a] Amit Basu and Steve Muylle. Authentication in e-commerce. *Communications of the Association for Computing Machinery*, 46(12): 159–166, December 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Blomer:2003:NPK

[BM03b] Johannes Blömer and Alexander May. New partial key exposure attacks on RSA. In Boneh [Bon03], pages 27–43. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Boyd:2003:PAK

[BM03c] Colin Boyd and Anish Mathuria. *Protocols for Authentication and Key Establishment*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 3-662-09527-0 (e-book), 3-642-07716-1. ISSN 1619-7100 (print), 2197-845X (electronic). xxiv + 323 pp. LCCN QA76.9.A25. URL http://www.springerlink.com/content/978-3-662-09527-0.

Burke:2000:ASFa

[BMA00a] Jerome Burke, John McDonald, and Todd Austin. Architectural support for fast symmetric-key cryptography. *ACM SIGARCH Computer Architecture News*, 28(5):178–189, December 2000. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Burke:2000:ASFb

[BMA00b] Jerome Burke, John McDonald, and Todd Austin. Architectural support for fast symmetric-key cryptography. *Operating Systems Review*, 34(5):178–189, December 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Burke:2000:ASFc

[BMA00c] Jerome Burke, John McDonald, and Todd Austin. Architectural support for fast symmetric-key cryptography. *ACM SIGPLAN Notices*, 35(11):178–189, November 2000. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Boneh:2000:GRK

[BMK00] Dan Boneh, Nagendra Modadugu, and Michael Kim. Generating RSA keys on a handheld using an untrusted server. *Lecture Notes in Computer Science*, 1977:271–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1977/19770271.htm; http://link.springer-ny.com/link/service/series/0558/papers/1977/19770271.pdf.

Biehl:2000:DFA

[BMM00] Ingrid Biehl, Bernd Meyer, and Volker Müller. Differential fault attacks on elliptic curve cryptosystems. In Bellare [Bel00], pages 131–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800131.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800131.pdf.

Boyd:2001:ECB

[BMN01] Colin Boyd, Paul Montague, and Khanh Nguyen. Elliptic curve based password authenticated key exchange protocols. *Lecture Notes in Computer Science*, 2119:487–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:

//link.springer-ny.com/link/service/series/0558/bibs/2119/21190487.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190487.pdf.

Boyko:2000:PSP

[BMP00] Victor Boyko, Philip MacKenzie, and Sarvar Patel. Provably secure password-authenticated key exchange using Diffie–Hellman. *Lecture Notes in Computer Science*, 1807:156–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070156.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070156.pdf.

Boneh:2003:SSS

[BMS03] Dan Boneh, Ilya Mironov, and Victor Shoup. A secure signature scheme from bilinear maps. In Joye [Joy03b], pages 98–110. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Buchmann:2006:PCL

[BMV06] Johannes Buchmann, Alexander May, and Ulrich Vollmer. Perspectives for cryptographic long-term security. *Communications of the Association for Computing Machinery*, 49(9):50–55, September 2006. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Borselius:2002:VTS

[BMW02a] Niklas Borselius, Chris J. Mitchell, and Aaron Wilson. On the value of threshold signatures. *Operating Systems Review*, 36(4):30–35, October 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Borselius:2002:PAU

[BMW02b] Niklas Borselius, Chris J. Mitchell, and Aaron Wilson. A pragmatic alternative to undetachable signatures. *Operating Systems Review*, 36(2):6–11, April 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Boyen:2005:DCC

[BMW05] Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identity-based techniques. In Meadows and Syverson [MS05b], pages 320–329. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Bellare:2000:AER

[BN00a] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, volume 1976 of *Lecture Notes in Comput. Sci.*, pages 531–545. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760531.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760531.pdf`.

Boneh:2000:TC

[BN00b] Dan Boneh and Moni Naor. Timed commitments. In Bellare [Bel00], pages 236–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800236.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800236.pdf`.

Bellare:2002:TSB

[BN02] Mihir Bellare and Gregory Neven. Transitive signatures based on factoring and RSA. *Lecture Notes in Computer Science*, 2501: 397–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2501/25010397.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010397.pdf`.

Bouganim:2008:DAC

[BNP08] Luc Bouganim, François Dang Ngoc, and Philippe Pucheral. Dynamic access-control policies on XML encrypted data. *ACM Transactions on Information and System Security*, 10(4):4:1–4:??, January 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bellare:2002:PRI

[BNPS02] Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. The power of RSA inversion oracles and the security of chaum's RSA-based blind signature scheme. *Lecture Notes in Computer Science*, 2339:319–??, 2002. CO-

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2339/23390319.htm; http://link.springer-ny.com/link/service/series/0558/papers/2339/23390319.pdf.

Bouganim:2003:CSD

[BNPW03] Luc Bouganim, François Dang Ngoc, Philippe Pucheral, and Lilan Wu. Chip-secured data access: Reconciling access rights with data encryption. In Freytag et al. [FLA+03], pages 1133–1136. ISBN 0-12-722442-4. LCCN ???? URL http://www.vldb.org/dblp/db/indices/a-tree/b/Bouganim:Luc.html.

Bodycombe:1999:CC

[Bod99] David J. Bodycombe. *Codes & ciphers*. Robinson, London, UK, 1999. ISBN 1-85487-897-2. vi + 122 pp. LCCN ????

Ben-Or:2005:UCS

[BOHL+05] Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In Kilian [Kil05], pages 386–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Bollinger:2002:UFO

[Bol02] Terry Bollinger. Use of Free and Open-Source Software (FOSS) in the U.S. Department of Defense: Version: 1.2. Mitre report MP 02 W0000101, MITRE Corporation, October 28, 2002. 160 pp. URL http://www.egovos.org/pdf/dodfoss.pdf.

Bondi:2000:CVB

[Bon00] Richard Bondi. *Cryptography for Visual Basic: a programmer's guide to the Microsoft CryptoAPI*. John Wiley and Sons, Inc., New York, NY, USA, 2000. ISBN 0-471-38189-6 (paperback). xx + 459 pp. LCCN QA76.73.B3 B665 2000.

Boneh:2001:SOR

[Bon01] Dan Boneh. Simplified OAEP for the RSA and Rabin functions. In Kilian [Kil01a], pages 275–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139.

UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390275.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390275.pdf.

Boneh:2003:ACC

[Bon03] Dan Boneh, editor. *Advances in Cryptology— CRYPTO 2003: 23rd Annual International Cryptology Conference Santa Barbara, California, USA, August 17–21, 2003 Proceedings*, volume 2729 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Boneh:2007:BLP

[Bon07] D. Boneh. A brief look at pairings based cryptography. In IEEE [IEE07], pages 19–26. ISBN 0-7695-3010-9. ISSN 0272-5428. LCCN QA76 .S974 2007. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4389466. IEEE Computer Society order number P3010.

Boone:2005:BHC

[Boo05] J. V. Boone. *A brief history of cryptology*. Naval Institute Press, Annapolis, MD, USA, 2005. ISBN 1-59114-084-6. xi + 192 pp. LCCN TK5102.85 .B66 2005. URL http://www.loc.gov/catdir/toc/ecip055/2005000009.html.

Borras:2000:TRT

[Bor00] Kevin Borras. A transport revolution: Turkey gets the smart card bug. *Toll-trans*, pages 36–38, September 2000.

Boreale:2001:STA

[Bor01] Michele Boreale. Symbolic trace analysis of cryptographic protocols. *Lecture Notes in Computer Science*, 2076:667–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2076/20760667.htm; http://link.springer-ny.com/link/service/series/0558/papers/2076/20760667.pdf.

Barak:2003:DC

[BOV03] Boaz Barak, Shien Jin Ong, and Salil Vadhan. Derandomization in cryptography. In Boneh [Bon03], pages 299–315. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817`.

Barak:2007:DC

[BOV07] Boaz Barak, Shien Jin Ong, and Salil Vadhan. Derandomization in cryptography. *SIAM Journal on Computing*, 37(2):380–400, ???? 2007. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Boyd:2001:ACA

[Boy01] Colin Boyd, editor. *Advances in cryptology — ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9–13, 2001: proceedings*, volume 2248 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-42987-5 (paperback). LCCN QA76.9.A25 I555 2001. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2248.htm`.

Boyen:2003:MIB

[Boy03] Xavier Boyen. Multipurpose identity-based signcryption: a Swiss Army knife for identity-based cryptography. In Boneh [Bon03], pages 383–399. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817`.

Bedi:2001:CNF

[BP01a] S. S. Bedi and N. R. Pillai. Cryptanalysis of the nonlinear FeedForward generator. *Lecture Notes in Computer Science*, 2247: 188–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470188.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470188.pdf.

Burnett:2001:RSO

[BP01b] Steve Burnett and Stephen Paine. *RSA Security's Official Guide to Cryptography*. McGraw-Hill, New York, NY, USA, 2001. ISBN 0-07-213139-X. xxi + 419 pp. LCCN TK5105.59.B87 200. US$59.99. Includes CD-ROM.

Bellare:2002:GSI

[BP02] Mihir Bellare and Adriana Palacio. GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In Yung [Yun02a], pages 162–177. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Barbancho:2003:CAC

[BP03a] A. M. Barbancho and A. Peinado. Cryptanalysis of anonymous channel protocol for large-scale area in wireless communications. *Computer Networks (Amsterdam, Netherlands: 1999)*, 43(6):777–785, December 20, 2003. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Buchbinder:2003:LUB

[BP03b] Niv Buchbinder and Erez Petrank. Lower and upper bounds on obtaining history independence. In Boneh [Bon03], pages 445–462. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Bellare:2004:KEA

[BP04] Mihir Bellare and Adriana Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In Franklin [Fra04], pages 273–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Blanchet:2005:VCP

[BP05] Bruno Blanchet and Andreas Podelski. Verification of cryptographic protocols: tagging enforces termination. *Theoretical Computer Science*, 333(1–2):67–90, March 1, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Beissinger:2006:CUM

[BP06] Janet Beissinger and Vera Pless. *The Cryptoclub: Using Mathematics to Make and Break Secret Codes*. A. K. Peters, Ltd., Wellesley, MA, USA, 2006. ISBN 1-56881-223-X. xvi + 199 pp. LCCN QA40.5 .B45 2006. URL http://www.loc.gov/catdir/toc/ecip067/2006002743.html.

Baer:2007:CIS

[BP07] Walter S. Baer and Andrew Parkinson. Cyberinsurance in IT security management. *IEEE Security & Privacy*, 5(3):50–56, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Bellare:2000:AKE

[BPR00] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. *Lecture Notes in Computer Science*, 1807: 139–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070139.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070139.pdf.

Borst:2001:CSC

[BPR01] Johan Borst, Bart Preneel, and Vincent Rijmen. Cryptography on smart cards. *Computer Networks (Amsterdam, Netherlands: 1999)*, 36(4):423–435, July 16, 2001. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.elsevier.nl/gej-ng/10/15/22/61/28/29/abstract.html; http://www.elsevier.nl/gej-ng/10/15/22/61/28/29/article.pdf.

Bellare:2005:ISA

[BPR05] Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC MACs. In Shoup [Sho05a], pages

527–454. ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621`.

Boneh:2008:IBI

[BPR+08] D. Boneh, P. Papakonstantinou, C. Rackoff, Y. Vahlis, and B. Waters. On the impossibility of basing identity based encryption on trapdoor permutations. In IEEE [IEE08], pages 283–292. ISBN 0-7695-3436-8. ISSN 0272-5428. LCCN QA76 .S95 2008. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=4690923`. IEEE Computer Society order number P3436.

Baudron:2000:ENS

[BPS00] Olivier Baudron, David Pointcheval, and Jacques Stern. Extended notions of security for multicast public key cryptosystems. *Lecture Notes in Computer Science*, 1853:499–511, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1853/18530499.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1853/18530499.pdf`.

Backes:2008:KDM

[BPS08] Michael Backes, Birgit Pfitzmann, and Andre Scedrov. Key-dependent message security under active attacks — BRSIM/UC-soundness of Dolev–Yao-style encryption with key cycles. *Journal of Computer Security*, 16(5):497–530, ???? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Benerecetti:2002:VST

[BPST02] Massimo Benerecetti, Maurizio Panti, Luca Spalazzi, and Simone Tacconi. Verification of the SSL/TLS protocol using a model checkable logic of belief and time. *Lecture Notes in Computer Science*, 2434: 126–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2434/24340126.htm`; `http://link.springer.de/link/service/series/0558/papers/2434/24340126.pdf`.

Brandao:2001:UEC

[BQR01] T. Brandão, M. P. Queluz, and A. Rodrigues. On the use of error correction codes in spread spectrum based image watermarking. *Lecture Notes in Computer Science*, 2195: 630–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950630.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950630.pdf.

Bellare:2000:ETE

[BR00a] Mihir Bellare and Phillip Rogaway. Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. In *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, volume 1976 of *Lecture Notes in Comput. Sci.*, pages 317–330. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760317.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760317.pdf.

Black:2000:CMA

[BR00b] John Black and Phillip Rogaway. CBC MACs for arbitrary-length messages:the three-key constructions. In Bellare [Bel00], pages 197–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800197.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800197.pdf.

Black:2001:CAF

[BR01] John Black and Phillip Rogaway. Ciphers with arbitrary finite domains. *Lecture Notes in Computer Science*, 2271:114–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710114.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710114.pdf.

Black:2002:BCM

[BR02] John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. *Lecture Notes in Computer Science*, 2332: 384–??, 2002. CODEN LNCSD9. ISSN 0302-

9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320384.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320384.pdf.

Bellare:2004:CBG

[BR04] M. Bellare and P. Rogaway. Code-based game-playing proofs and the security of triple encryption. Cryptology ePrint Archive report 2004/331, 2004. URL http://eprint.iacr.org/2004/331.

Bugliesi:2005:NIP

[BR05] Michele Bugliesi and Sabina Rossi. Non-interference proof techniques for the analysis of cryptographic protocols. *Journal of Computer Security*, 13(1):87–113, ???? 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bellare:2006:MPP

[BR06] Mihir Bellare and Thomas Ristenpart. Multi-property-preserving hash domain extension and the EMD transform. In ????, editor, *Advances in Cryptology — ASIACRYPT 2006*, pages 299–314. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN ???? LCCN ???? URL ????.

Bhatnagar:2009:RRW

[BR09] Gaurav Bhatnagar and Balasubramanian Raman. Robust reference-watermarking scheme using wavelet packet transform and bidiagonal-singular value decomposition. *International Journal of Image and Graphics (IJIG)*, 9(3):449–477, July 2009. CODEN ???? ISSN 0219-4678.

Brands:2001:RPK

[Bra01a] Stefan A. Brands. *Rethinking public key infrastructures and digital certificates: building in privacy*. MIT Press, Cambridge, MA, USA, 2001. ISBN 0-262-02491-8. xxi + 314 pp. LCCN TK5105.59 .B73 2000.

Brandt:2001:CPS

[Bra01b] Felix Brandt. Cryptographic protocols for secure second-price auctions. *Lecture Notes in Computer Science*, 2182: 154–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2182/21820154.htm; http://link.springer-ny.com/link/service/series/0558/papers/2182/21820154.pdf.

Brackenridge:2006:IUU

[Bra06] B. Brackenridge. Invention: Ultrawideband upset. *IEEE Spectrum*, 43 (9):65–66, September 2006. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Brown:2005:CEC

[Bro05a] Christopher L. T. Brown. *Computer evidence: collection and preservation*. Charles River Media, Hingham, MA, USA, 2005. ISBN 1-58450-405-6 (pbk. with cd-rom). ???? pp. LCCN HV8079.C65 B76 2005. URL http://www.loc.gov/catdir/toc/ecip0514/2005016674.html.

Browne:2005:DEP

[Bro05b] Graham T. Browne. *Data encryption: a practical guide to protecting sensitive information*. Aaben Kryptografi, Cranage, UK, 2005. ISBN 0-9549513-0-1. ???? pp. LCCN ???? One CD-ROM.

Black:2002:BBA

[BRS02] John Black, Phillip Rogaway, and Thomas Shrimpton. Black-box analysis of the block-cipher-based hash-function constructions from PGV. In Yung [Yun02a], pages 320–335. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420320.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420320.pdf.

Butler:2009:LIB

[BRTM09] Kevin R. B. Butler, Sunam Ryu, Patrick Traynor, and Patrick D. McDaniel. Leveraging identity-based cryptography for node ID assignment in structured P2P systems. *IEEE Transactions on Parallel and Distributed Systems*, 20(12):1803–1815, December 2009. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Brustoloni:2006:LEN

[Bru06] José Carlos Brustoloni. Laboratory experiments for network security instruction. *ACM Journal on Educational Resources in Computing (JERIC)*, 6(4):5:1–5:??, December 2006. CODEN ???? ISSN 1531-4278.

Bierbrauer:2000:AIW

[BS00a] Jürgen Bierbrauer and Holger Schellwat. Almost independent and weakly biased arrays: Efficient constructions and cryptologic applications. In Bellare [Bel00], pages 533–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800533.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800533.pdf.

Biryukov:2000:CTM

[BS00b] Alex Biryukov and Adi Shamir. Cryptanalytic time/memory/data tradeoffs for stream ciphers. *Lecture Notes in Computer Science*, 1976:1–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760001.pdf.

Barrett:2001:SSS

[BS01a] Daniel J. Barrett and Richard E. Silverman. *SSH: The Secure Shell: The Definitive Guide*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, 2001. ISBN 0-596-00011-1. xv + 540 pp. LCCN QA76.76.O63 B369 2001. US$39.95. URL http://www.oreilly.com/catalog/9780596000110; http://www.oreilly.com/catalog/sshtdg/; http://www.snailbook.com/.

Bigun:2001:AVB

[BS01b] Josef Bigun and Fabrizio Smeraldi, editors. *Audio- and video-based biometric person authentication: Third International Conference, AVBPA 2001, Halmstad, Sweden, June 6–8, 2001: Proceedings*, volume 2091 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-42216-1 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.S65 .A944 2001; QA267.A1 L43 no.2091. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2091.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2091.

Biryukov:2001:SCS

[BS01c] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. *Lecture Notes in Computer Science*, 2045:394–405, 2001. CODEN LNCSD9. ISSN

0302-9743 (print), 1611-3349 (electronic).

Boneh:2001:UBE

[BS01d] Dan Boneh and Igor E. Shparlinski. On the unpredictability of bits of the elliptic curve Diffie–Hellman scheme. In Kilian [Kil01a], pages 201–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390201.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390201.pdf.

Banks:2002:NSR

[BS02] William D. Banks and Igor E. Shparlinski. On the number of sparse RSA exponents. *Journal of Number Theory*, 95(2):340–350, August 2002. CODEN JNUTA9. ISSN 0022-314X (print), 1096-1658 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022314X01927751.

Bajard:2003:ISC

[BS03] Jean Claude Bajard and Michael Schulte, editors. *16th IEEE Symposium on Computer Arithmetic: ARITH-16 2003: proceedings: Santiago de Compostela, Spain, June 15–18, 2003*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2003. ISBN 0-7695-1894-X. ISSN 1063-6889. LCCN ???? URL http://www.dec.usc.es/arith16/. IEEE order no. PR01894.

Barrett:2005:SSS

[BSB05] Daniel J. Barrett, Richard E. Silverman, and Robert G. Byrnes. *SSH: The Secure Shell: The Definitive Guide*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, second edition, 2005. ISBN 0-596-00895-3. 672 (est.) pp. LCCN QA76.76.O63 B369 2001. US$39.95. URL http://www.oreilly.com/catalog/9780596008956; http://www.oreilly.com/catalog/sshtdg2/.

Bo:2001:EID

[BSC01a] Xiaochen Bo, Lincheng Shen, and Wensen Chang. Evaluation of the image degradation for a typical watermarking algorithm in the block-DCT domain. *Lecture Notes in Computer Science*, 2229:52–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:

//link.springer-ny.com/link/service/series/0558/bibs/2229/22290052.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290052.pdf.

Bo:2001:SCD

[BSC01b] Xiaochen Bo, Lincheng Shen, and Wensen Chang. Sign correlation detector for blind image watermarking in the DCT domain. *Lecture Notes in Computer Science*, 2195:780–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950780.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950780.pdf.

Bounkong:2002:ICA

[BSL02] Stéphane Bounkong, David Saad, and David Lowe. Independent component analysis for domain independent watermarking. *Lecture Notes in Computer Science*, 2415:510–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2415/24150510.htm; http://link.springer-ny.com/link/service/series/0558/papers/2415/24150510.pdf.

Brisbane:2000:RBW

[BSNO00] Gareth Brisbane, Rei Safavi-Naini, and Philip Ogunbona. Region-based watermarking by distribution adjustment. *Lecture Notes in Computer Science*, 1975:54–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750054.htm; http://link.springer-ny.com/link/service/series/0558/papers/1975/19750054.pdf.

Bresson:2002:TRS

[BSS02] Emmanuel Bresson, Jacques Stern, and Michael Szydlo. Threshold ring signatures and applications to ad-hoc groups. In Yung [Yun02a], pages 465–480. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420465.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420465.pdf.

Blake:2004:AEC

[BSS04] Ian F. Blake, G. (Gadiel) Seroussi, and Nigel P. (Nigel Paul) Smart, editors. *Advances in elliptic curve cryptography*, volume 317 of *London Mathematical Society lecture note series*. Cambridge University Press, Cambridge, UK, 2004. ISBN 0-521-60415-X. xvi + 281 pp. LCCN QA76.9.A25 A375 2004. URL `http://www.loc.gov/catdir/description/cam051/2004054519.html; http://www.loc.gov/catdir/toc/cam051/2004054519.html`.

Blake:2005:AEC

[BSS05] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Advances in elliptic curve cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, UK, second edition, April 2005. ISBN 0-521-60415-X. xvi + 281 pp. LCCN QA76.9.A25 A375 2004. URL `http://www.cambridge.org/us/academic/subjects/mathematics/number-theory/advances-elliptic-curve-cryptography`.

Bhargav-Spantzel:2007:PPM

[BSSM+07] Abhilasha Bhargav-Spantzel, Anna C. Squicciarini, Shimon Modi, Matthew Young, Elisa Bertino, and Stephen J. Elliott. Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, 15(5):529–560, ???? 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Buchmann:2002:ICP

[BST02] Johannes Buchmann, Kouichi Sakurai, and Tsuyoshi Takagi. An IND-CCA2 public-key cryptosystem with fast decryption. *Lecture Notes in Computer Science*, 2288: 51–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880051.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880051.pdf`.

Barak:2003:TRN

[BST03] Boaz Barak, Ronen Shaltiel, and Eran Tromer. True random number generators secure in a changing environment. In Walter et al. [WKP03], pages 166–180. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http:`

//www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Biryukov:2001:RTC

[BSW01] Alex Biryukov, Adi Shamir, and David Wagner. Real time cryptanalysis of A5/1 on a PC. *Lecture Notes in Computer Science*, 1978: 1–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780001.pdf.

Bethencourt:2009:NTP

[BSW09] John Bethencourt, Dawn Song, and Brent Waters. New techniques for private stream searching. *ACM Transactions on Information and System Security*, 12(3):16:1–16:??, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Biehl:2002:NDP

[BT02] Ingrid Biehl and Tsuyoshi Takagi. A new distributed primality test for shared RSA keys using quadratic fields. *Lecture Notes in Computer Science*, 2384: 1–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840001.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840001.pdf.

Boyer:2002:LDS

[BTTF02] John Boyer, Andrew D. Todd, Jason Trenough, and Doug Farrell. Letters: Defective sign-and-encrypt and healthcare woes and J2EE cache and pool and Regex++. *Dr. Dobb's Journal of Software Tools*, 27 (2):10, February 2002. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Beimel:2005:CIW

[BTW05] Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. In Kilian [Kil05], pages 600–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=

3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Beimel:2008:CIW

[BTW08] Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. *SIAM Journal on Discrete Mathematics*, 22(1):360–397, ???? 2008. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Black:2002:SCA

[BU02] John Black and Hector Urtubia. Side-channel attacks on symmetric encryption schemes: The case for authenticated encryption. In USENIX [USE02b], pages 327–338. ISBN 1-931971-00-5. LCCN ???? URL http://www.usenix.org/publications/library/proceedings/sec02/black.html.

Buchmann:2000:CTC

[Buc00a] Johannes Buchmann, editor. *Coding theory, cryptography, and related areas: proceedings of an International Conference on Coding Theory, Cryptography, and Related Areas, held in Guanajuato, Mexico, in April 1998.* Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-66248-0 (softcover). LCCN TK5102.94 .I58 1998. URL http://www.springer.com/mathematics/numbers/book/978-3-540-66248-8.

Buchmann:2000:IC

[Buc00b] Johannes Buchmann. *Introduction to Cryptography*. Undergraduate texts in mathematics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 0-387-95034-6. xi + 281 pp. LCCN QA268.B83 2001. UK£29.50.

Buchmann:2001:IC

[Buc01] Johannes Buchmann. *Introduction to cryptography*. Undergraduate texts in mathematics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 0-387-95034-6 (hardcover). xi + 281 pp. LCCN QA268.B83 2001.

Buchmann:2004:IC

[Buc04] Johannes Buchmann. *Introduction to cryptography*. Undergraduate texts in mathematics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2004. ISBN 0-387-20756-2 , 0-387-21156-X. xvi + 335 pp. LCCN QA268.B83; QA268.B83 2004.

Budiansky:2000:BWC

[Bud00a] Stephen Budiansky. *Battle of Wits: The Complete Story of Codebreaking in World War II*. Free Press, New York, NY, USA, 2000. ISBN 0-684-85932-7. 436 pp. LCCN D810.C88 B83 2000. US$27.50, UK£20.

Budiansky:2000:DBU

[Bud00b] Stephen Budiansky. The difficult beginnings of US–British codebreaking cooperation. *Intelligence and National Security*, 15(2):49–??, 2000. ISSN 0268-4527 (print), 1743-9019 (electronic).

Budiansky:2002:BWC

[Bud02] Stephen Budiansky. *Battle of wits: the complete story of codebreaking in World War II*. Simon and Schuster, New York, NY, USA, 2002. ISBN 0-7432-1734-9 (paperback). 436 + 16 pp. LCCN ???? US$16.00.

Budiansky:2006:HMS

[Bud06] Stephen Budiansky. *Her Majesty's spymaster: Elizabeth I, Sir Francis Walsingham, and the birth of modern espionage*. Plume, New York, NY, USA, 2006. ISBN 0-452-28747-2. xvii + 235 + 8 pp. LCCN DA358.W2 B83 2006.

Buhan:2006:FBL

[Buh06] Ileana Buhan. Feeling is believing: a location limited channel based on grip pattern biometrics and cryptanalysis. CTIT technical report 06-29, Centre for Telematics and Information Technology, University of Twente, Enschede, The Netherlands, 2006. 10 pp.

Bulygin:2009:PSS

[Bul09] Stanislav Bulygin. *Polynomial system solving for decoding linear codes and algebraic cryptanalysis*. Ph.D. thesis (??), Technische Universität Kaiserslautern, Kaiserslautern, Germany, 2009.

Burmansson:2000:TCY

[Bur00] Frank Burmansson. Travel cards in the year 2000: the Helsinki region ushers in the smart card era. *Urban public transportation systems*, pages 229–238, Engineers 2000.

Burnett:2001:CB

[Bur01] Steve Burnett. Crypto blunders, 2001. URL `http://db.usenix.org/publications/library/proceedings/lisa2001/tech/`. Unpublished invited talk, LISA 2001: 15th Systems Administration Conference, December 2–7, 2001, Town and Country Resort Hotel, San Diego, CA.

Burke:2002:IWA

[Bur02] Colin B. Burke. *It wasn't all magic: the early struggle to automate cryptanalysis, 1930s–1960s*, volume 6 of *United States cryptologic history special series*. Center for Cryptologic History, National Security Agency, Fort George G. Meade, MD, USA, 2002. 344 pp. LCCN Z103.4. U6. URL http://archive.org/details/NSA-WasntAllMagic_2002; http://purl.fdlp.gov/GPO/gpo40404; http://purl.stanford.edu/jj264fh4943; http://www.nsa.gov/public_info/_files/cryptologic_histories/magic.pdf.

Burr:2003:SAE

[Bur03] William E. Burr. Selecting the Advanced Encryption Standard. *IEEE Security & Privacy*, 1(2):43–52, March/April 2003. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://dlib.computer.org/sp/books/sp2003/pdf/j2043.pdf; http://www.computer.org/security/j2043abs.htm.

Burr:2006:CHS

[Bur06] William E. Burr. Cryptographic hash standards: Where do we go from here? *IEEE Security & Privacy*, 4(2):88–91, March/April 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Boesgaard:2004:RNH

[BVP+04] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius. Rabbit: a new high performance stream cipher. In ????, editor, *Proceedings of Fast Software Encryption 10*, volume 2887, pages 307–329. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004.

Baker:2007:ISU

[BW07] Wade H. Baker and Linda Wallace. Is information security under control?: Investigating quality in information security management. *IEEE Security & Privacy*, 5(1):36–44, January/February 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Blake-Wilson:2002:RUE

[BWBL02] S. Blake-Wilson, D. Brown, and P. Lambert. RFC 3278: Use of Elliptic Curve Cryptography (ECC) algorithms in Cryptographic Message Syntax (CMS), April 2002. URL ftp://ftp.internic.net/rfc/rfc3278.txt; https://www.math.utah.edu/pub/rfc/rfc3278.txt.

Butler:2000:NSA

[BWE+00] Randy Butler, Von Welch, Douglas Engert, Ian Foster, Steven Tuecke, John Volmer, and Carl Kesselman. A national-scale authentication infrastructure. *Computer*, 33(12):60–66, December 2000. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co2000/pdf/rz060.pdf`; `http://www.computer.org/computer/co2000/rz060abs.htm`.

Bellare:2003:FSP

[BY03] Mihir Bellare and Bennet Yee. Forward-security in private-key cryptography. In Joye [Joy03b], pages 1–18. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612`.

Bar-Yossef:2004:ESQ

[BYJK04] Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In ACM [ACM04b], pages 128–137. ISBN 1-58113-852-0. LCCN QA75.5 .A22 2004.

Bar-Yossef:2008:ESQ

[BYJK08] Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *SIAM Journal on Computing*, 38(1):366–384, ???? 2008. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Bertlmann:2002:QUB

[BZ02] Reinhold A. Bertlmann and Anton Zeilinger, editors. *Quantum [Un]speakables: From Bell to Quantum Information: Conference in Commemoration of the Physicist John S. Bell, 10–14 November 2000, Vienna*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. ISBN 3-540-42756-2. LCCN ????

Bond:2003:DTA

[BZ03] Mike Bond and Piotr Zieliński. Decimalisation table attacks for PIN cracking. Technical Report 560, University of Cambridge Computer Laboratory, Cambridge, UK, February 2003. 14 pp. URL `http://www.cl.cam.`

ac.uk/TechReports/UCAM-CL-TR-560.pdf.

Borders:2005:CHP

[BZP05] Kevin Borders, Xin Zhao, and Atul Prakash. CPOL: high-performance policy evaluation. In Meadows and Syverson [MS05b], pages 147–157. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Carrington:2002:EDS

[C$^+$02] Charles Carrington et al., editors. *Enterprise directory and security implementation guide: designing and implementing directories in your organization*. Academic Press, New York, NY, USA, 2002. ISBN 0-12-160452-7. xxvi + 238 pp. LCCN HD9696.25.A2 E58 2002. US$49.95.

Staff:2003:NTC

[CAC03] CACM Staff. News track: Cinematic watermark; eye-opening education; roaming time; stand by me; savings bonds fade to net; phone home. *Communications of the Association for Computing Machinery*, 46(7):9–10, July 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Staff:2006:NTS

[CAC06] CACM Staff. News track: Super game plan; E-learning roots disputed; Chinese history; U.K. seeks popular science input; encryption commitment; *Improve*-ment news; vid kid. *Communications of the Association for Computing Machinery*, 49 (11):9–10, November 2006. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

CALACIT:2000:SID

[Cal00a] California Legislature.Assembly Committee on Information Technology. *Securing the Internet: digital signatures and electronic transactions in California*. Sacramento, CA, August 4, 2000. various pp.

CADOJ:2000:DSE

[Cal00b] California.Dept.of Justice. *Digital signature, election petitions, public and private transactions: initiative statute*. Elections Division, October 13, 2000. 15 pp. Title and summary prepared by the California Attorney General. Initiative #905.

CAMTC:2000:TSC

[Cal00c] California.Metropolitan Transportation Commission. TransLink smart card: universal transit card for the San Francisco Bay Area. Technical report, Metropolitan Transportation Commission, Oakland, CA, 2000. 4 pp.

Caloyannides:2000:EWE

[Cal00d] M. A. Caloyannides. Encryption wars: early battles. *IEEE Spectrum*, 37(4): 37–43, April 2000. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Caloyannides:2000:EWS

[Cal00e] M. A. Caloyannides. Encryption wars: shifting tactics. *IEEE Spectrum*, 37(5): 46–51, May 2000. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Calvocoressi:2001:TSU

[Cal01] Peter Calvocoressi. *Top secret Ultra*. M and M Baldwin, Cleobury Mortimer, Kidderminster, England, 2001. ISBN 0-947712-41-0. 158 pp. LCCN D810.C88 C34 2001.

Canetti:2001:UCS

[Can01a] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In IEEE [IEE01a], pages 136–145. CODEN ASFPDV. ISBN 0-7695-1390-5, 0-7695-1391-3 (case), 0-7695-1392-1 (microfiche). ISSN 0272-5428. LCCN ????

Canteaut:2001:CFD

[Can01b] A. Canteaut. Cryptographic functions and design criteria for block ciphers. *Lecture Notes in Computer Science*, 2247:1–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470001.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470001.pdf`.

Canetti:2006:SCC

[Can06a] Ran Canetti. Security and composition of cryptographic protocols: a tutorial (part I). *ACM SIGACT News*, 37(3):67–92, September 2006. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL `http://doi.acm.org/10.1145/1165555.1165570`.

Canteaut:2006:OPR

[Can06b] Anne Canteaut. Open problems related to algebraic attacks on stream ciphers. In Ytrehus [Ytr06], pages 120–134. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Caprara:2001:PSR

[Cap01] Alberto Caprara. On the practical solution of the reversal median problem. *Lecture Notes in Computer Science*, 2149: 238–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2149/21490238.htm; http://link.springer-ny.com/link/service/series/0558/papers/2149/21490238.pdf.

Carriere:2000:PSC

[Car00] Bruno Carriere. Le passe sans contact: autopsie d'une puce. *La vie du rail et des transports*, pages 43–48, November 2000.

Carter:2001:SCT

[Car01] Amy Carter. Smart card technology just got smarter. *Metro*, 97(9), December 2001.

Carlet:2002:LCC

[Car02] Claude Carlet. A larger class of cryptographic Boolean functions via a study of the Maiorana–McFarland construction. In Yung [Yun02a], pages 549–564. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420549.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420549.pdf.

Casey:2002:HCC

[Cas02] Eoghan Casey, editor. *Handbook of computer crime investigation: forensic tools and technology*. Academic Press, New York, NY, USA, 2002. ISBN 0-12-163103-6. xiv + 448 pp. LCCN HV8079.C65 H36 2002. US$39.95.

Cass:2003:LES

[Cas03] Stephen Cass. Listening in [electronic spying]. *IEEE Spectrum*, 40(4):32–37, April 2003. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Casselman:2006:MTE

[Cas06] Bill Casselman. Mathematical theory of the Enigma machine. *Notices of the American Mathematical Society*, 53(4):433, April 2006. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL http://www.mathaware.org/; http://www.nationalarchives.gov.uk/; http://www.turingarchive.org/browse.php/C/30. The front cover of this issue displays eight pages of Alan Turing's description of the Enigma machine. The issue is a special tribute to Kurt Gödel for the centenary of his birth.

Cobas:2001:CTA

[CB01] Juan David González Cobas and José Antonio López Brugos. A complexity-theoretic approach to the design of good measures of cryptographic strength. *Lecture Notes in Computer Science*, 2178:233–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2178/21780233.htm; http://link.springer-ny.com/link/service/series/0558/papers/2178/21780233.pdf.

Challal:2005:HHC

[CBB05] Yacine Challal, Abdelmadjid Bouabdallah, and Hatem Bettahar. H_2A: Hybrid hash-chaining scheme for adaptive multicast source authentication of media-streaming. *Computers & Security*, 24(1):57–68, February 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001816.

Cooper:2005:AAP

[CBD+05] Brian F. Cooper, Mayank Bawa, Neil Daswani, Sergio Marti, and Hector Garcia-Molina. Authenticity and availability in PIPE networks. *Future Generation Computer Systems*, 21(3): 391–400, March 1, 2005. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Chandramouli:2006:BPA

[CBSU06] R. Chandramouli, S. Bapatla, K. P. Subbalakshmi, and R. N. Uma. Battery power-aware encryption. *ACM Transactions on Information and System Security*, 9(2):162–180, May 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cachin:2000:OFS

[CC00] Christian Cachin and Jan Camenisch. Optimistic fair secure computation. In Bellare [Bel00], pages 93–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800093.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800093.pdf.

Chan:2001:CRP

[CC01a] Chi-Kwong Chan and L. M. Cheng. Cryptanalysis of a remote password authentication scheme. *International Journal of Computer Mathematics*, 78(3):

323–326, 2001. CODEN IJCMAT. ISSN 0020-7160.

Chan:2001:CTB

[CC01b] Chi-Kwong Chan and L. M. Cheng. Cryptanalysis of a timestamp-based password authentication scheme. *Computers & Security*, 21(1):74–76, First Quarter 2001. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404802001104.

Carline:2002:NWT

[CC02a] Dylan Carline and Paul Coulton. A novel watermarking technique for LUT based FPGA designs. *Lecture Notes in Computer Science*, 2438: 1152–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2438/24381152.htm; http://link.springer-ny.com/link/service/series/0558/papers/2438/24381152.pdf.

Chan:2002:SLI

[CC02b] Chi-Kwong Chan and L. M. Cheng. Security of Lin's image watermarking system. *The Journal of Systems and Software*, 62(3): 211–215, June 15, 2002. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Cachin:2004:ACE

[CC04a] Christian Cachin and Jan Camenisch, editors. *Advances in Cryptology— EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2–6, 2004: Proceedings*, volume 3027 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-21935-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://link.springer-ny.com/link/service/series/0558/tocs/t3027.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3027; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b97182.

Chang:2004:SES

[CC04b] Ya-Fen Chang and Chin-Chen Chang. A secure and efficient strong-password authentication protocol. *Operating Systems Review*, 38(3):79–90, July 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Cousot:2004:AIB

[CC04c] Patrick Cousot and Radhia Cousot. An abstract interpretation-based framework for software watermarking. *ACM SIGPLAN Notices*, 39(1):173–185, January 2004. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Chan:2005:STM

[CC05a] Chao-Wen Chan and Chin-Chen Chang. A scheme for threshold multi-secret sharing. *Applied Mathematics and Computation*, 166(1):1–14, July 6, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2005:ASN

[CC05b] Ya-Fen Chang and Chin-Chen Chang. Authentication schemes with no verification table. *Applied Mathematics and Computation*, 167(2):820–832, August 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2005:EAP

[CC05c] Ya-Fen Chang and Chin-Chen Chang. An efficient authentication protocol for mobile satellite communication systems. *Operating Systems Review*, 39(1):70–84, January 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Comon:2005:TAO

[CC05d] Hubert Comon and Véronique Cortier. Tree automata with one memory set constraints and cryptographic protocols. *Theoretical Computer Science*, 331(1):143–214, February 15, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Crandall:2005:SAM

[CC05e] Jedidiah R. Crandall and Frederic T. Chong. A security assessment of the Minos architecture. *ACM SIGARCH Computer Architecture News*, 33(1):48–57, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Chuang:2006:USF

[CC06] J.-C. Chuang and C.-C. Chang. Using a simple and fast image compression algorithm to hide secret information. *International Journal of Computer Applications*, 28(4):329–333, 2006. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https:`

//www.tandfonline.com/doi/full/10.1080/1206212X.2006.11441818.

Chen:2008:SNI

[CC08] Chien-Chang Chen and Yu-Wei Chien. Sharing numerous images secretly with reduced possessing load. *Fundamenta Informaticae*, 86 (4):447–458, October 2008. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Chang:2009:FDI

[CC09] Chin-Chen Chang and Yung-Chen Chou. A fragile digital image authentication scheme inspired by wet paper codes. *Fundamenta Informaticae*, 90(1–2):17–26, January 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Chan:2001:WEF

[CCCY01] Alvin T. S. Chan, Jiannong Cao, Henry Chan, and Gilbert Young. A Web-enabled framework for smart card applications in health services. *Communications of the Association for Computing Machinery*, 44(9):76–82, September 2001. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/articles/journals/cacm/2001-44-9/p76-chan/p76-chan.pdf; http://www.acm.org/pubs/citations/journals/cacm/2001-44-9/p76-chan/.

Collberg:2004:DPB

[CCD+04] C. Collberg, E. Carter, S. Debray, A. Huntwork, J. Kececioglu, C. Linn, and M. Stepp. Dynamic path-based software watermarking. *ACM SIGPLAN Notices*, 39(6):107–118, May 2004. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Cimato:2006:UMU

[CCD06] Stelvio Cimato, Antonella Cresti, and Paolo D'Arco. A unified model for unconditionally secure key distribution. *Journal of Computer Security*, 14(1):45–64, ???? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chai:2007:EIB

[CCD07] Zhenchuan Chai, Zhenfu Cao, and Xiaolei Dong. Efficient ID-based multi-receiver threshold decryption. *International Journal of Foundations of Computer Science (IJFCS)*, 18 (5):987–1004, October 2007. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Cattaneo:2001:DIT

[CCDP01] Giuseppe Cattaneo, Luigi Catuogno, Aniello Del Sorbo, and Pino Persiano. The design and implementation of a transparent cryptographic file system for UNIX. In USENIX [USE01b], page ?? ISBN 1-880446-10-3. LCCN QA76.8.U65 U84 2001. URL http://www.usenix.org/publications/library/proceedings/usenix01/freenix01/cattaneo.html.

Chen:2004:TPM

[CCH04] Tzer-Shyong Chen, Yu-Fang Chung, and Kuo-Hsuan Huang. A traceable proxy multisignature scheme based on the elliptic curve cryptosystem. *Applied Mathematics and Computation*, 159(1):137–145, November 25, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2005:DSM

[CCH05] Ya-Fen Chang, Chin-Chen Chang, and Hui-Feng Huang. Digital signature with message recovery using self-certified public keys without trustworthy system authority. *Applied Mathematics and Computation*, 161(1): 211–227, February 4, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2004:IDA

[CCK04a] Ya-Fan Chang, Chin-Chen Chang, and Chia-Lin Kao. An improvement on a deniable authentication protocol. *Operating Systems Review*, 38(3):65–74, July 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chang:2004:SOT

[CCK04b] Ya-Fen Chang, Chin-Chen Chang, and Jui-Yi Kuo. A secure one-time password authentication scheme using Smart Cards without limiting login times. *Operating Systems Review*, 38(4):80–90, October 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chang:2009:PCC

[CCL09] Chin-Chen Chang, Tzung-Her Chen, and Li-Jen Liu. Preventing cheating in computational visual cryptography. *Fundamenta Informaticae*, 92(1–2):27–42, January 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Christianson:2001:PKC

[CCM01] Bruce Christianson, Bruno Crispo, and James A. Malcolm. Public-key cryptosystems using symmetric-key crypto-algorithms. *Lec-*

ture Notes in Computer Science, 2133:182–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330182.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330182.pdf.

Choi:2005:JMA

[CCM05] Hyung-Kyu Choi, Yoo C. Chung, and Soo-Mook Moon. Java memory allocation with lazy worst fit for small objects. *The Computer Journal*, 48(4):437–442, July 2005. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/48/4/437; http://comjnl.oxfordjournals.org/cgi/reprint/48/4/437.

Christianson:2002:SPI

[CCMR02] Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors. *Security Protocols: 9th International Workshop Cambridge, UK, April 25–27, 2001. Revised Papers*, volume 2467 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-44263-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 S443 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2467.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2467.

Christianson:2005:SPI

[CCMR05] Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors. *Security Protocols: 11th International Workshop, Cambridge, UK, April 2–4, 2003, Revised Selected Papers*, volume 3364 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-28389-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3364.

Castelluccia:2009:EPS

[CCMT09] Claude Castelluccia, Aldar C-F. Chan, Einar Mykletun, and Gene Tsudik. Efficient and provably secure aggregation of encrypted data in wireless sensor networks. *ACM Transactions on Sensor Networks*, 5(3): 20:1–20:??, May 2009. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Chen:2008:NMA

[CCS08] Yalin Chen, Jue-Sam Chou, and Hung-Min Sun. A novel mutual authentication scheme based on quadratic residues for RFID systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 52(12):2373–2380, August 22, 2008. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Caboara:2008:GBP

[CCT08] Massimo Caboara, Fabrizio Caruso, and Carlo Traverso. Gröbner bases for public key cryptography. In Jeffrey [Jef08], pages 315–324. ISBN 1-59593-904-0. LCCN ????

Choi:2002:IPP

[CCW02] Dug-Hwan Choi, Seungbok Choi, and Dongho Won. Improvement of probabilistic public key cryptosystems using discrete logarithm. *Lecture Notes in Computer Science*, 2288: 72–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880072.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880072.pdf`.

Camenisch:2000:VEG

[CD00a] Jan Camenisch and Ivan Damgård. Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes (extended abstract). In *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, volume 1976 of *Lecture Notes in Comput. Sci.*, pages 331–345. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760331.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760331.pdf`.

Carpenter:2000:CB

[CD00b] Mary Carpenter and Betty Paul Dowse. The code breakers of 1942. *Wellesley*, ??(??):26–30, Winter 2000.

Cramer:2001:SDL

[CD01a] Ronald Cramer and Ivan Damgård. Secure distributed linear algebra in a constant number of rounds.

In Kilian [Kil01a], pages 119–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390119.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390119.pdf.

Crouch:2001:LAR

[CD01b] P. A. Crouch and J. H. Davenport. Lattice attacks on RSA-encrypted IP and TCP. *Lecture Notes in Computer Science*, 2260:329–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600329.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600329.pdf.

Cramer:2000:CVS

[CDD00] Ronald Cramer, Ivan Damgård, and Stefan Dziembowski. On the complexity of verifiable secret sharing and multiparty computation. In ACM [ACM00], pages 325–334. ISBN 1-58113-184-4. URL http://www.acm.org/pubs/articles/proceedings/stoc/335305/p325-cramer/p325-cramer.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/335305/p325-cramer/. ACM order number 508000.

Ceselli:2005:MAI

[CDD+05] Alberto Ceselli, Ernesto Damiani, Sabrina De Capitani Di Vimercati, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Modeling and assessing inference exposure in encrypted databases. *ACM Transactions on Information and System Security*, 8(1):119–152, February 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cimato:2007:CVC

[CDD07] S. Cimato, R. De Prisco, and A. De Santis. Colored visual cryptography without color darkening. *Theoretical Computer Science*, 374(1–3):261–276, April 20, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Cramer:2001:CRS

[CDF01] Ronald Cramer, Ivan Damgård, and Serge Fehr. On the cost of reconstructing a secret, or VSS with optimal reconstruction phase. In Kilian [Kil01a], pages 503–?? ISBN 3-540-42456-3 (paperback). LCCN

QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390503.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390503.pdf.

Cimato:2005:ICV

[CDFM05] Stelvio Cimato, Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Ideal contrast visual cryptography schemes with reversing. *Information Processing Letters*, 93(4):199–206, February 28, 2005. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Cramer:2005:CMS

[CDG+05] Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, and Carles Padró. On codes, matroids and secure multiparty computation from linear secret sharing schemes. In Shoup [Sho05a], pages 327–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Cramer:2005:SCP

[CDI05] Ronald Cramer, Ivan Damgård, and Yuval Ishai. Share conversion, pseudorandom secret-sharing and applications to secure computation. In Kilian [Kil05], pages 342–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Cavallar:2000:FBR

[CDL+00] Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman te Riele, Karen Aardal, Jeff Gilchrist, Gérard Guillerm, Paul Leyland, Joël Marchand, François Morain, Alec Muffett, Chris Putnam, Craig Putnam, and Paul Zimmermann. Factorization of a 512-bit RSA modulus. *Lecture Notes in Computer Science*, 1807:1–18, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:

//link.springer-ny.com/link/service/series/0558/bibs/1807/18070001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070001.pdf.

Cortier:2006:SAP

[CDL06] Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1): 1–43, ???? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cramer:2000:GSM

[CDM00] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multi-party computation from any linear secret-sharing scheme. *Lecture Notes in Computer Science*, 1807:316–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070316.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070316.pdf.

Chawla:2005:TPP

[CDM+05] Shuchi Chawla, Cynthia Dwork, Frank McSherry, Adam Smith, and Hoeteck Wee. Toward privacy in public databases. In Kilian [Kil05], pages 363–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Coron:2005:MDR

[CDMP05] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle–Damgård revisited: How to construct a hash function. In Shoup [Sho05a], pages 430–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Cramer:2001:MCT

[CDN01] Ronald Cramer, Ivan Damgård, and Jesper B. Nielsen. Multiparty computation from threshold homomorphic encryption. In *Advances in cryptology—EUROCRYPT*

2001 (Innsbruck), volume 2045 of *Lecture Notes in Comput. Sci.*, pages 280–300. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450280.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450280.pdf`.

Chapman:2001:PEA

[CDR01] Mark Chapman, George I. Davida, and Marc Rennhard. A practical and effective approach to large-scale automated linguistic steganography. *Lecture Notes in Computer Science*, 2200: 156–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2200/22000156.htm; http://link.springer-ny.com/link/service/series/0558/papers/2200/22000156.pdf`.

Castiglione:2007:TAD

[CDS07] A. Castiglione, A. De Santis, and C. Soriente. Taking advantages of a disadvantage: Digital forensics and steganography using document metadata. *The Journal of Systems and Software*, 80(5):750–764, May 2007. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Chen:2005:NVW

[CDTT05] Zhenyong Chen, Junhui Deng, Long Tang, and Zesheng Tang. A novel video watermarking resistant to spatio-temporal desynchronization. In Han et al. [HYZ05b], pages 532–?? ISBN 981-270-153-2. LCCN ???? URL `http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html`.

Ceravolo:2004:ERH

[Cer04a] P. Ceravolo. Extracting role hierarchies from authentication data flows. *International Journal of Computer Systems Science and Engineering*, 19(3):??, May 2004. CODEN CSSEEI. ISSN 0267-6192.

Certicom:2004:CCC

[Cer04b] *Code & Cipher: Certicom's Bulletin of Security and Cryptography*, 2004. URL `http://www.certicom.com/codeandcipher`. Certicom, 5520 Explorer Drive, 4th Floor Mississauga, Ontario, L4W 5L1 Canada. Published quarterly.

Canetti:2001:UCC

[CF01a] Ran Canetti and Marc Fischlin. Universally composable commitments. In Kilian [Kil01a], pages 19–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390019.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390019.pdf.

Canteaut:2001:COR

[CF01b] Anne Canteaut and Eric Filiol. Ciphertext only reconstruction of stream ciphers based on combination generators. *Lecture Notes in Computer Science*, 1978:165–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780165.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780165.pdf.

Cramer:2002:OBB

[CF02] Ronald Cramer and Serge Fehr. Optimal black-box secret sharing over arbitrary Abelian groups. In Yung [Yun02a], pages 272–287. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420272.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420272.pdf.

Clarke:2005:AUM

[CF05] N. L. Clarke and S. M. Furnell. Authentication of users on mobile telephones — a survey of attitudes and practices. *Computers & Security*, 24(7):519–527, October 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404805001446.

Clarke:2007:AUA

[CF07] N. L. Clarke and S. M. Furnell. Advanced user authentication for mobile devices. *Computers & Security*, 26(2):109–119, March 2007. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404806001428.

Cohen:2006:HEH

[CFA+06] Henri Cohen, Gerhard Frey, Roberto Avanzi, et al., editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, 2006. ISBN 1-58488-518-1. xxxiv + 808 pp. LCCN QA567.2.E44 H36 2006. URL http://www.loc.gov/catdir/enhancements/fy0647/2005041841-d.html.

Clarke:2002:ASA

[CFRR02] N. L. Clarke, S. M. Furnell, P. M. Rodwell, and P. L. Reynolds. Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security*, 21(3):220–228, June 1, 2002. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404802003048.

Courtois:2001:HAM

[CFS01] Nicolas T. Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. *Lecture Notes in Computer Science*, 2248: 157–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480157.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480157.pdf.

Cramer:2005:BBS

[CFS05] Ronald Cramer, Serge Fehr, and Martijn Stam. Black-box secret sharing from primitive sets in algebraic number fields. In Shoup [Sho05a], pages 344–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Climent:2006:NEC

[CFVZ06] Joan-Josep Climent, Francisco Ferrández, José-Francisco Vicent, and Antonio Zamora. A nonlinear elliptic curve cryptosystem based on matrices. *Applied Mathematics and Computation*, 174 (1):150–164, March 1, 2006. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2010:PRN

[CFY+10] Weiling Chang, Binxing Fang, Xiaochun Yun, Shupeng Wang, and Xiangzhan Yu. A pseudo-random number generator based on LZSS. In *2010 Data Compression Conference (DCC)*, page 524. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5453503.

Chodowiec:2003:VCF

[CG03] Paweł Chodowiec and Kris Gaj. Very compact FPGA implementation of the AES algorithm. In Walter et al. [WKP03], pages 319–333. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Cranor:2005:SUD

[CG05] Lorrie Faith Cranor and Simson Garfinkel. *Security and usability: designing secure systems that people can use*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, 2005. ISBN 0-596-00827-9 (paperback). xviii + 714 pp. LCCN QA76.9.A25; QA76.9.A25 S3533 2005; QA76.9.A25 S43 2005eb; QA76.9.A25 S43 2005. US$44.95, CDN$62.95, UK£31.95.

Candebat:2006:SPM

[CG06] Thibault Candebat and David Gray. Secure pseudonym management using mediated identity-based encryption. *Journal of Computer Security*, 14(3):249–267, ???? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chodowiec:2001:ETG

[CGBS01] Pawel Chodowiec, Kris Gaj, Peter Bellows, and Brian Schott. Experimental testing of the Gigabit IPSec-compliant implementations of Rijndael and Triple DES using SLAAC-1V FPGA accelerator board. *Lecture Notes in Computer Science*, 2200:220–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2200/22000220.htm; http://link.springer-ny.com/link/service/series/0558/papers/2200/22000220.pdf.

Caballero-Gil:2009:GBA

[CGFSHG09] P. Caballero-Gil, A. Fúster-Sabater, and C. Hernández-Goya. Graph-based approach to the edit distance cryptanalysis of irregularly clocked linear feedback shift registers. *J.UCS: Journal of Universal Computer Science*, 15(15):2981–??, ???? 2009. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_15_15/graph_based_approach_to.

Catalano:2000:CIS

[CGH00a] Dario Catalano, Rosario Gennaro, and Shai Halevi. Computing inverses over a shared secret modulus. *Lecture Notes in Computer Science*, 1807: 190–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070190.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070190.pdf.

Coppersmith:2000:ICT

[CGH+00b] Don Coppersmith, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M. Matyas, Jr., Mohammad Peyravian, David Safford, and Nevenko Zunic. IBM comments: Third AES Conference April 13, 2000. In NIST [NIS00], pages 333–336. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Catalano:2001:BSP

[CGHG01] Dario Catalano, Rosario Gennaro, and Nick Howgrave-Graham. The bit security of Paillier's encryption scheme and its applications. In *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 229–243. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450229.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450229.pdf.

Caballero-Gil:2006:SSB

[CGHG06] P. Caballero-Gil and C. Hernández-Goya. Secret sharing based on a hard-on-average problem. *Linear Algebra and* *its Applications*, 414(2–3): 626–631, April 15, 2006. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic).

Crosby:2002:CHB

[CGJ+02] Scott Crosby, Ian Goldberg, Robert Johnson, Dawn Song, and David Wagner. A cryptanalysis of the high-bandwidth digital content protection system. *Lecture Notes in Computer Science*, 2320:192–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2320/23200192.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2320/23200192.pdf`.

Clarke:2002:UCP

[CGK+02] Dwaine Clarke, Blaise Gassend, Thomas Kotwal, Matt Burnside, Marten van Dijk, Srinivas Devadas, and Ronald Rivest. The untrusted computer problem and camera-based authentication. *Lecture Notes in Computer Science*, 2414: 114–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2414/24140114.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2414/24140114.pdf`.

Chen:2008:OVBa

[CGL+08a] Xiaoxin Chen, Tal Garfinkel, E. Christopher Lewis, Pratap Subrahmanyam, Carl A. Waldspurger, Dan Boneh, Jeffrey Dwoskin, and Dan R. K. Ports. Overshadow: a virtualization-based approach to retrofitting protection in commodity operating systems. *ACM SIGARCH Computer Architecture News*, 36(1):2–13, March 2008. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Chen:2008:OVBb

[CGL+08b] Xiaoxin Chen, Tal Garfinkel, E. Christopher Lewis, Pratap Subrahmanyam, Carl A. Waldspurger, Dan Boneh, Jeffrey Dwoskin, and Dan R. K. Ports. Overshadow: a virtualization-based approach to retrofitting protection in commodity operating systems. *Operating Systems Review*, 42(2): 2–13, March 2008. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chen:2008:OVBc

[CGL+08c] Xiaoxin Chen, Tal Garfinkel, E. Christopher Lewis, Pratap

Subrahmanyam, Carl A. Waldspurger, Dan Boneh, Jeffrey Dwoskin, and Dan R. K. Ports. Overshadow: a virtualization-based approach to retrofitting protection in commodity operating systems. *ACM SIGPLAN Notices*, 43(3):2–13, March 2008. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Caballero-Gil:2007:PSC

[CGM07] Pino Caballero-Gil and Gerasimos C. Meletiou. Preface of the symposium 15: Cryptology, information security, and networks. In Simos and Maroulis [SM07b], pages 935–936. ISBN 0-7354-0476-3 (set), 0-7354-0477-1 (vol. 1), 0-7354-0478-X (vol. 2). ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. LCCN Q183.9 .I524 2007. URL `http://proceedings.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf& id=APCPCS000963000002000935000001& idtype=cvips`.

Canovas:2002:DSB

[CGMM02] Óscar Cánovas, Antonio F. Gómez, Humberto Martínez, and Gregorio Martínez. Different Smartcard-based approaches to physical access control. *Lecture Notes in Computer Science*, 2437: 214–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2437/24370214.htm; http://link.springer.de/link/service/series/0558/papers/2437/24370214.pdf`.

Cox:2002:SP9

[CGP+02] Russ Cox, Eric Grosse, Rob Pike, Dave Presotto, and Sean Quinlan. Security in Plan 9. In USENIX [USE02b], pages 3–16. ISBN 1-931971-00-5. LCCN ???? URL `http://plan9.bell-labs.com/sys/doc/auth.pdf; http://www.usenix.org/publications/library/proceedings/sec02/cox.html`.

Cimato:2003:SCN

[CGP03] Stelvio Cimato, Clemente Galdi, and Guiseppe Persiano, editors. *Security in communication networks: Third International Conference, SCN 2002, Amalfi, Italy, September 11–13, 2002: Revised Papers*, volume 2576 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-00420-3 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK5105.59 .S385 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2576.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2576. Also available via the World Wide Web.

Cayrel:2008:SIS

[CGP08] P.-L. Cayrel, P. Gaborit, and E. Prouff. Secure implementation of the Stern authentication and signature schemes. *Lecture Notes in Computer Science*, 5189: 191–205, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chow:2009:ADN

[CGV09] Stanley T. Chow, Christophe Gustave, and Dmitri Vinokurov. Authenticating displayed names in telephony. *Bell Labs Technical Journal*, 14(1):267–282, Spring 2009. CODEN BLTJFD. ISSN 1089-7089 (print), 1538-7305 (electronic).

Crotch-Harvey:2000:OPR

[CH00] Trevor Crotch-Harvey. Operators are poised to reap smart card benefits. *International railway journal and rapid transit review: IRJ*, 40 (2):31–32, February 2000.

Chang:2001:TFG

[CH01a] Chin-Chen Chang and Kuo-Feng Hwang. Towards the forgery of a group signature without knowing the group center's secret. *Lecture Notes in Computer Science*, 2229:47–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290047.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290047.pdf.

Chen:2001:SFW

[CH01b] Minghua Chen and Yun He. A synchronous fragile watermarking scheme for erroneous Q–DCT coefficients detection. *Lecture Notes in Computer Science*, 2195:812–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950812.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950812.pdf.

Chien:2007:SUL

[CH07a] Hung-Yu Chien and Chen-Wei Huang. Security of ultra-lightweight RFID authentication protocols and its improvements. *Operating Systems Review*, 41(4): 83–86, July 2007. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chung:2007:ASF

[CH07b] Jaewook Chung and M. Anwar Hasan. Asymmetric squaring formulae. In Kornerup and Muller [KM07], pages 113–122. ISBN 0-7695-2854-6. ISSN 1063-6889. LCCN ???? URL http://www.lirmm.fr/arith18/.

Chung:2007:MRA

[CH07c] Jaewook Chung and M. Anwar Hasan. Montgomery reduction algorithm for modular multiplication using low-weight polynomial form integers. In Kornerup and Muller [KM07], pages 230–239. ISBN 0-7695-2854-6. ISSN 1063-6889. LCCN ???? URL http://www.lirmm.fr/arith18/.

Chaum:2004:VSB

[Cha04] David Chaum. E-voting: Secret-ballot receipts: True voter-verifiable elections. *IEEE Security & Privacy*, 2(1):38–47, January/February 2004. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://csdl.computer.org/comp/mags/sp/2004/01/j1038abs.htm; http://csdl.computer.org/dl/mags/sp/2004/01/j1038.pdf.

Chan:2005:MCM

[Cha05a] Alvin T. S. Chan. Mobile cookies management on a smart card. *Communications of the Association for Computing Machinery*, 48 (11):38–43, November 2005. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Chandra:2005:BWS

[Cha05b] Praphul Chandra. *Bulletproof wireless security: GSM, UMTS, 802.11 and ad hoc security*. Communications engineering series. Newnes Press, Amsterdam, The Netherlands and Boston, MA, USA, 2005. ISBN 0-7506-7746-5 (paperback). xxxiii + 237 pp. LCCN TK5103.2 .C445 2005. URL http://books.elsevier.com/us/mk/us/subindex.asp?isbn=0750677465.

Chakrabarti:2007:GCS

[Cha07] Anirban Chakrabarti. *Grid computing security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-44492-0 (hardcover). xiv + 331 pp. LCCN QA76.9.C58 C53 2007.

Chang:2001:NEA

[CHC01] Chin-Chen Chang, Min-Shian Hwang, and Tung-

Shou Chen. A new encryption algorithm for image cryptosystems. *The Journal of Systems and Software*, 58(2):83–91, September 1, 2001. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.elsevier.com/gej-ng/10/29/11/68/33/27/abstract.html`.

Chen:2004:MCK

[CHC04] Tzer-Shyong Chen, Kuo-Hsuan Huang, and Yu-Fang Chung. Modified cryptographic key assignment scheme for overcoming the incorrectness of the CHW scheme. *Applied Mathematics and Computation*, 159 (1):147–155, November 25, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chen:2005:EUG

[CHC05] Tzer-Shyong Chen, Jen-Yan Huang, and Tzer-Long Chen. An efficient undeniable group-oriented signature scheme. *Applied Mathematics and Computation*, 165(1):95–102, June 6, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chen:2000:JCT

[Che00a] Zhiqun Chen. *Java Card technology for Smart Cards: architecture and programmer's guide*. Java series. Addison-Wesley, Reading, MA, USA, 2000. ISBN 0-201-70329-7. xxii + 368 pp. LCCN QA76.73.J38 C478 2000.

Cherry:2000:SLD

[Che00b] S. Cherry. Secrets and lies: digital security in a networked world [books]. *IEEE Spectrum*, 37(10):15–16, October 2000. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Chen:2001:DEU

[Che01a] Chaur-Chin Chen. Data encryption using MRF with an RSA key. *Lecture Notes in Computer Science*, 2195:399–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950399.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2195/21950399.pdf`.

Chen:2001:PDP

[Che01b] Su-Shing Chen. The paradox of digital preservation. *Computer*, 34(3):24–28, March 2001. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co2001/pdf/r3024.pdf`;

http://www.computer.org/computer/co2001/r3024abs.htm.

Cheon:2001:NVR

[Che01c] Jung Hee Cheon. Nonlinear vector resilient functions. In Kilian [Kil01a], pages 458–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390458.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390458.pdf.

Cherry:2001:HMH

[Che01d] S. M. Cherry. Hyperencryption: Much hype about little that is new [web sites]. *IEEE Spectrum*, 38(4):87, April 2001. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Cherry:2001:HDS

[Che01e] S. M. Cherry. Is hyperlinking to decryption software illegal? *IEEE Spectrum*, 38(8):64–65, August 2001. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Cherry:2001:REM

[Che01f] S. M. Cherry. Remailers elude e-mail surveillance. *IEEE Spectrum*, 38(11):69, November 2001. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Chen:2002:SFS

[Che02] Yangjun Chen. Signature files and signature trees. *Information Processing Letters*, 82(4):213–221, May 31, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Cheng:2003:PPO

[Che03] Qi Cheng. Primality proving via one round in ECPP and one iteration in AKS. In Boneh [Bon03], pages 338–348. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Chen:2004:IAM

[Che04a] Bi-Hui Chen. Improvement of authenticated multiple-key agreement protocol. *Operating Systems Review*, 38 (3):35–41, July 2004. CO-

DEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Cheng:2004:BSD

[Che04b] Qi Cheng. On the bounded sum-of-digits discrete logarithm problem in finite fields. In Franklin [Fra04], pages 201–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Chen:2005:TSS

[Che05a] Tzer-Shyong Chen. A threshold signature scheme based on the elliptic curve cryptosystem. *Applied Mathematics and Computation*, 162(3):1119–1134, March 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Cherry:2005:MDC

[Che05b] S. Cherry. My dad's computer: a conservation with Internet security expert William R. Cheswick. *IEEE Spectrum*, 42(8):55–56, August 2005. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Chess:2005:SAC

[Che05c] David M. Chess. Security in autonomic computing. *ACM SIGARCH Computer Architecture News*, 33(1):2–5, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Chen:2007:CIS

[Che07a] Wen-Yuan Chen. Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation. *Applied Mathematics and Computation*, 185(1):432–448, February 1, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Cherry:2007:MEV

[Che07b] S. Cherry. Making every e-vote count. *IEEE Spectrum*, 44(1):13–14, January 2007. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Chen:2008:CIS

[Che08a] Wen-Yuan Chen. Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. *Applied Mathematics and Computation*, 196(1):40–54, February 15, 2008. CODEN AMHCBQ.

ISSN 0096-3003 (print), 1873-5649 (electronic).

Chen:2008:MWS

[Che08b] Wen-Yuan Chen. Multiple-watermarking scheme of the European Article Number Barcode using similar code division multiple access technique. *Applied Mathematics and Computation*, 197(1):243–261, March 15, 2008. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Coulter:2001:GAH

[CHH01] Robert S. Coulter, George Havas, and Marie Henderson. Giesbrecht's algorithm, the HFE cryptosystem and Ore's p^s-polynomials. In *Computer mathematics (Matsuyama, 2001)*, volume 9 of *Lecture Notes Ser. Comput.*, pages 36–45. World Scientific Publishing Co., Singapore; Philadelphia, PA, USA; River Edge, NJ, USA, 2001.

Choi:2009:KDK

[CHH+09] Seung Geol Choi, Javier Herranz, Dennis Hofheinz, Jung Yeon Hwang, Eike Kiltz, Dong Hoon Lee, and Moti Yung. The Kurosawa–Desmedt key encapsulation is not chosen-ciphertext secure. *Information Processing Letters*, 109(16):897–901, July 31, 2009. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chien:2008:EPA

[Chi08a] H. Y. Chien. Efficient and practical approach to authenticating public terminals. *International Journal of Computer Applications*, 30(4):319–324, 2008. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2008.11441911`.

Chien:2008:PAUa

[Chi08b] Hung-Yu Chien. Practical anonymous user authentication scheme with security proof. *Computers & Security*, 27(5–6):216–223, October 2008. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404808000291`.

Chien:2008:PAUb

[Chi08c] Hung-Yu Chien. Practical anonymous user authentication scheme with security proof. *Computers & Security*, 27(5–6):216–223, October 2008. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404808000291`.

Chien:2008:PAUc

[Chi08d] Hung-Yu Chien. Practical anonymous user authentication scheme with security proof. *Computers & Security*, 27(5–6):216–223, October 2008. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808000291.

Chien:2008:SCA

[Chi08e] Hung-Yu Chien. Selectively convertible authenticated encryption in the random oracle model. *The Computer Journal*, 51(4):419–434, July 2008. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/51/4/419; http://comjnl.oxfordjournals.org/cgi/content/full/51/4/419; http://comjnl.oxfordjournals.org/cgi/reprint/51/4/419.

Coron:2001:GGC

[CHJ+01a] Jean-Sébastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, and Christophe Tymen. GEM: a Generic chosen-ciphertext secure Encryption Method. *Lecture Notes in Computer Science*, 2271:263–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710263.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710263.pdf.

Coron:2001:OCC

[CHJ+01b] Jean-Sébastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, and Christophe Tymen. Optimal chosen-ciphertext secure encryption of arbitrary-length messages. *Lecture Notes in Computer Science*, 2274:17–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740017.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740017.pdf.

Coppersmith:2002:CSC

[CHJ02] Don Coppersmith, Shai Halevi, and Charanjit Jutla. Cryptanalysis of stream ciphers with linear masking. In Yung [Yun02a], pages 515–532. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http:/

/link.springer.de/link/service/series/0558/bibs/2442/24420515.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420515.pdf.

Canetti:2003:FSP

[CHK03] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. *Lecture Notes in Computer Science*, 2656:255–271, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_16.pdf.

Canetti:2005:ASN

[CHK05] Ran Canetti, Shai Halevi, and Jonathan Katz. Adaptively-secure, non-interactive public-key encryption. In Kilian [Kil05], pages 150–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Cheon:2008:PST

[CHKO08] Jung Hee Cheon, Nicholas Hopper, Yongdae Kim, and Ivan Osipkov. Provably Secure Timed-Release Public Key Encryption. *ACM Transactions on Information and System Security*, 11(2):4:1–4:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chang:2002:IBO

[CHL02] Yan-Cheng Chang, Chun-Yun Hsiao, and Chi-Jen Lu. On the impossibilities of basing one-way permutations on central cryptographic primitives. *Lecture Notes in Computer Science*, 2501:110–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010110.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010110.pdf.

Chao:2009:HCS

[ChLYL09] Min-Wen Chao, Chao hung Lin, Cheng-Wei Yu, and Tong-Yee Lee. A high capacity 3D steganography algorithm. *IEEE Transactions on Visualization and Computer Graphics*, 15(2):274–284, March/April 2009. CODEN ITVGEA. ISSN 1077-2626 (print), 1941-0506 (electronic), 2160-9306.

Chen:2002:CPK

[CHM+02] L. Chen, K. Harrison, A. Moss, D. Soldera, and N. P. Smart. Certification of public keys within an identity based system. *Lecture Notes in Computer Science*, 2433:322–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330322.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330322.pdf.

Choi:2006:CHP

[Cho06] Su-Jeong Choi. *Cryptanalysis of a homomorphic public-key cryptosystem*. Thesis (Ph.D.), University of London, London, UK, 2006. ???? pp.

Choo:2008:PLP

[Cho08a] Kim-Kwang Raymond Choo. Privacy on the line: The politics of wiretapping and encryption, updated and expanded edition. *The Computer Journal*, 51(6):744, November 2008. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/full/51/6/744; http://comjnl.oxfordjournals.org/cgi/reprint/51/6/744.

Chowdhury:2008:CBG

[Cho08b] Milton M. Chowdhury. *Cryptanalysis of braid group based protocols*. Thesis (MPhil), Faculty of Engineering and Physical Sciences, University of Manchester, Manchester, UK, 2008. 230 pp.

Christianson:2000:SPI

[Chr00] Bruce Christianson, editor. *Security protocols: 7th International Workshop, Cambridge, UK, April 19–21, 1999: Proceedings*, volume 1796 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. CODEN LNCSD9. ISBN 3-540-67381-4 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1796. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1796.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1796.

Christianson:2001:SPI

[Chr01] Bruce Christianson, editor. *Security protocols: 8th International Workshop, Cambridge, UK, April 3–5, 2000: Revised Papers*, volume 2133 of *Lecture Notes in Computer Science*.

Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-42566-7 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.2133. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2133.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2133.

Canetti:2005:HAW

[CHS05] Ran Canetti, Shai Halevi, and Michael Steiner. Hardness amplification of weakly verifiable puzzles. In Kilian [Kil05], pages 17–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Chen:2002:AMT

[CHSS02] L. Chen, K. Harrison, D. Soldera, and N. P. Smart. Applications of multiple trust authorities in pairing based cryptosystems. *Lecture Notes in Computer Science*, 2437: 260–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2437/24370260.htm; http://link.springer.de/link/service/series/0558/papers/2437/24370260.pdf.

Cornea:2002:SCI

[CHT02] Marius Cornea, John Harrison, and Ping Tak Peter Tang. *Scientific computing on Itanium-based systems.* Intel Corporation, Santa Clara, CA, USA, 2002. ISBN 0-9712887-7-1. xvii + 406 pp. LCCN QA76.8.I83 C67 2002. US$69.95. URL http://www.intel.com/intelpress/sum_scientific.htm.

Churchhouse:2002:CCJ

[Chu02] Robert F. Churchhouse. *Codes and Ciphers: Julius Caesar, the Enigma, and the Internet.* Cambridge University Press, Cambridge, UK, 2002. ISBN 0-521-81054-X (hardcover), 0-521-00890-5 (paperback). x + 240 pp. LCCN Z103 .C48 2002. US$55.00 (hardcover), US$20.00 (paperback).

Canvel:2003:PIS

[CHVV03] Brice Canvel, Alain Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password interception in a SSL/TLS channel. In Boneh [Bon03], pages 583–599. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Chang:2005:ILW

[CHY05a] Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang Yang. An improvement on the Lin–Wu (t, n) threshold verifiable multi-secret sharing scheme. *Applied Mathematics and Computation*, 163(1):169–178, April 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2005:NMS

[CHY05b] Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang Yang. A new multi-stage secret sharing scheme using one-way function. *Operating Systems Review*, 39(1):48–55, January 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Cimato:2002:DAP

[Cim02] Stelvio Cimato. Design of an authentication protocol for Gsm Javacards. *Lecture Notes in Computer Science*, 2288:355–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880355.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880355.pdf.

Cirstea:2001:SAP

[Cir01] Horatiu Cirstea. Specifying authentication protocols using rewriting and strategies. *Lecture Notes in Computer Science*, 1990:138–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1990/19900138.htm; http://link.springer-ny.com/link/service/series/0558/papers/1990/19900138.pdf.

Cheon:2003:PTA

[CJ03a] Jung Hee Cheon and Byungheup Jun. A polynomial time algorithm for the braid Diffie–Hellman conjugacy problem. In Boneh [Bon03], pages 212–225. CODEN LNCSD9.

ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Chien:2003:HAP

[CJ03b] Hung-Yu Chien and Jinn-Ke Jan. A hybrid authentication protocol for large mobile network. *The Journal of Systems and Software*, 67(2):123–130, August 15, 2003. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Chien:2003:NHA

[CJ03c] Hung-Yu Chien and Jinn-Ke Jan. New hierarchical assignment without public key cryptography. *Computers & Security*, 22(6):523–526, September 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803006138.

Chien:2003:RSA

[CJ03d] Hung-Yu Chien and Jinn-Ke Jan. Robust and simple authentication protocol. *The Computer Journal*, 46(2):193–201, February 2003. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_46/Issue_02/460193.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_46/Issue_02/pdf/460193.pdf.

Chien:2004:IAM

[CJ04] Hung-Yu Chien and Jinn-Ke Jan. Improved authenticated multiple-key agreement protocol without using conventional one-way function. *Applied Mathematics and Computation*, 147(2):491–497, January 12, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chen:2005:EDS

[CJ05] Yi-Hwa Chen and Jinn-Ke Jan. Enhancement of digital signature with message recovery using self-certified public keys and its variants. *Operating Systems Review*, 39(3):90–96, July 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Cornwall:2004:AAM

[CJK+04] Linda A. Cornwall, Jens Jensen, David P. Kelsey, Ákos Frohner, Daniel Kouřil, Franck Bonnassieux, Sophie Nicoud, Károly Lõrentey, Joni Hahkala, Mika Silander, Roberto Cecchini, Vincenzo Ciaschini, Luca dell'Agnello, Fabio Spataro, David O'Callaghan, Olle Mulmo, Gian Luca Volpato, David Groep, Martijn Steenbakkers, and Andrew McNab. Authentication and authorization mechanisms for multi-domain Grid environments. *Journal of Grid Computing*, 2(4):301–311, December 2004. CODEN ???? ISSN 1570-7873 (print), 1572-9184 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=1570-7873&volume=2&issue=4&spage=301`.

Choie:2005:EIB

[CJL05] Young Ju Choie, Eunkyung Jeong, and Eunjeong Lee. Efficient identity-based authenticated key agreement protocol from pairings. *Applied Mathematics and Computation*, 162(1):179–188, March 4, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chin:2006:HSI

[CJL06] Chong Siew Chin, Andrew Teoh Beng Jin, and David Ngo Chek Ling. High security Iris verification system based on random secret integration. *Computer Vision and Image Understanding: CVIU*, 102(2):169–177, May 2006. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic).

Clarke:2000:VSP

[CJM00] E. M. Clarke, S. Jha, and W. Marrero. Verifying security protocols with Brutus. *ACM Transactions on Software Engineering and Methodology*, 9(4):443–487, October 2000. CODEN ATSMER. ISSN 1049-331X (print), 1557-7392 (electronic). URL `http://www.acm.org/pubs/articles/journals/tosem/2000-9-4/p443-clarke/p443-clarke.pdf`; `http://www.acm.org/pubs/citations/journals/tosem/2000-9-4/p443-clarke/`.

Coron:2000:NAP

[CJNP00] Jean-Sébastien Coron, Marc Joye, David Naccache, and Pascal Paillier. New attacks on PKCS#1 v1.5 encryption. *Lecture Notes in Computer Science*, 1807:369–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070369.htm`; `http://link.springer-ny.com/link/service/series/`

0558/papers/1807/18070369.pdf.

Coron:2002:UPS

[CJNP02] Jean-Sébastien Coron, Marc Joye, David Naccache, and Pascal Paillier. Universal padding schemes for RSA. In Yung [Yun02a], pages 226–241. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420226.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420226.pdf.

Chepyzhov:2001:SAF

[CJS01] Vladimor V. Chepyzhov, Thomas Johansson, and Ben Smeets. A simple algorithm for fast correlation attacks on stream ciphers. *Lecture Notes in Computer Science*, 1978: 181–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780181.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780181.pdf.

Chien:2001:MRL

[CJT01] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng. A modified remote login authentication scheme based on geometric approach. *The Journal of Systems and Software*, 55(3): 287–290, January 15, 2001. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.elsevier.nl/gej-ng/10/29/11/54/27/29/abstract.html; http://www.elsevier.nl/gej-ng/10/29/11/54/27/29/article.pdf.

Chien:2002:EPS

[CJT02] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng. An efficient and practical solution to remote authentication: Smart card. *Computers & Security*, 21(4):372–375, August 1, 2002. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404802004157.

Chien:2003:CMV

[CJT03] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng. Cryptanalysis on Mu–Varadharajan's e-voting schemes. *Applied Mathematics and Computation*, 139(2–3):525–530, July 15, 2003. CODEN AMHCBQ. ISSN 0096-3003

(print), 1873-5649 (electronic).

Chien:2004:SIS

[CJT04] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng. Solving the invalid signer-verified signature problem and comments on Xia–You group signature. *The Journal of Systems and Software*, 73(3):369–373, November/ December 2004. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Canetti:2002:SAI

[CK02a] Ran Canetti and Hugo Krawczyk. Security analysis of IKE's signature-based key-exchange protocol. In Yung [Yun02a], pages 143–161. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL `http://link.springer.de/link/service/series/0558/bibs/2442/24420143.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420143.pdf`.

Canetti:2002:UCN

[CK02b] Ran Canetti and Hugo Krawczyk. Universally composable notions of key exchange and secure channels. *Lecture Notes in Computer Science*, 2332: 337–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320337.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320337.pdf`.

Cook:2006:CEG

[CK06] Debra Cook and Angelos Keromytis. *CryptoGraphics: Exploiting Graphics Cards for Security*, volume 25 of *Advances in information security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 0-387-29015-X. LCCN ???? US$99.00. URL `http://www.loc.gov/catdir/enhancements/fy0663/2006925092-d.html`.

Cheon:2002:IID

[CKK+02] Jung Hee Cheon, MunJu Kim, Kwangjo Kim, Jung-Yeun Lee, and SungWoo Kang. Improved impossible differential cryptanalysis of Rijndael and Crypton. *Lecture Notes in Computer Science*, 2288:39–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880039.htm; http://link.springer-`

ny.com/link/service/series/0558/papers/2288/22880039.pdf.

Chung:2003:EPX

[CKK03] Yon Dohn Chung, Jong Wook Kim, and Myoung Ho Kim. Efficient preprocessing of XML queries using structured signatures. *Information Processing Letters*, 87(5):257–264, September 15, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chun:2003:DLC

[CKL+03] Kilsoo Chun, Seungjoo Kim, Sangjin Lee, Soo Hak Sung, and Seonhee Yoon. Differential and linear cryptanalysis for 2-round SPNs. *Information Processing Letters*, 87(5):277–282, September 15, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Cox:2005:DWT

[CKL05] I. J. (Ingemar J.) Cox, Ton Kalker, and Heung-Kyu Lee, editors. *Digital watermarking: third international workshop, IWDW 2004, Seoul, Korea, October 30–November 1, 2004: revised selected papers*, volume 3304 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-24839-0 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I89 2004. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3304.

Chen:2009:SRP

[CKL+09] Yingying Chen, Konstantinos Kleisouris, Xiaoyan Li, Wade Trappe, and Richard P. Martin. A security and robustness performance analysis of localization algorithms to signal strength attacks. *ACM Transactions on Sensor Networks*, 5(1):2:1–2:??, February 2009. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Coppersmith:2000:KRF

[CKM00] Don Coppersmith, Lars R. Knudsen, and Chris J. Mitchell. Key recovery and forgery attacks on the MacDES MAC algorithm. In Bellare [Bel00], pages 184–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800184.htm; http://link.springer-ny.com/link/service/series/

0558/papers/1880/18800184.pdf.

Coron:2000:FLA

[CKN00] Jean-Sébastien Coron, François Koeune, and David Naccache. From fixed-length to arbitrary-length RSA padding schemes. *Lecture Notes in Computer Science*, 1976:90–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760090.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760090.pdf.

Coron:2001:SSL

[CKN01] Jean-Sébastien Coron, Paul Kocher, and David Naccache. Statistics and secret leakage. *Lecture Notes in Computer Science*, 1962:157–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620157.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620157.pdf.

Canetti:2003:RCC

[CKN03] Ran Canetti, Hugo Krawczyk, and Jesper B. Nielsen. Relaxing chosen-ciphertext security. In Boneh [Bon03], pages 565–582. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Cheon:2006:KPC

[CKN06] Jung Hee Cheon, Woo-Hwan Kim, and Hyun Soo Nam. Known-plaintext cryptanalysis of the Domingo–Ferrer algebraic privacy homomorphism scheme. *Information Processing Letters*, 97(3):118–123, February 14, 2006. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Cachin:2001:SEA

[CKPS01] Christian Cachin, Klaus Kursawe, Frank Petzold, and Victor Shoup. Secure and efficient asynchronous broadcast protocols. In Kilian [Kil01a], pages 524–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139.

UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390524.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390524.pdf.

Cathalo:2003:NTT

[CKQ03] Julien Cathalo, François Koeune, and Jean-Jacques Quisquater. A new type of timing attack: Application to GPS. In Walter et al. [WKP03], pages 291–303. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Chevalier:2008:CRS

[CKRT08] Yannick Chevalier, Ralf Küsters, Michaël Rusinowitch, and Mathieu Turuani. Complexity results for security protocols with Diffie–Hellman exponentiation and commuting public key encryption. *ACM Transactions on Computational Logic*, 9(4):24:1–24:??, August 2008. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Cachin:2009:TC

[CKS09] Christian Cachin, Idit Keidar, and Alexander Shraer. Trusting the cloud. *ACM SIGACT News*, 40(2):81–86, June 2009. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Chen:2005:CLR

[CKY05] Chien-Yuan Chen, Cheng-Yuan Ku, and David C. Yen. Cryptanalysis of large RSA exponent by using the LLL algorithm. *Applied Mathematics and Computation*, 169(1):516–525, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chen:2007:CRA

[CKY07] Chien-Yuan Chen, Cheng-Yuan Ku, and David C. Yen. Cryptographic relational algebra for databases using the field authenticator. *Computers and Mathematics with Applications*, 54(1):38–44, July 2007. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122107001721.

Chen:2000:IBD

[CL00] J. J.-R. Chen and Y. Liu. An ID-based digital multisignatures scheme with time stamp technique. *International Journal of Computer Systems Science and Engineering*, 15(2):105–??, March 2000. CODEN CSSEEI. ISSN 0267-6192.

Camenisch:2001:IES

[CL01a] Jan Camenisch and Anna Lysyanskaya. An identity escrow scheme with appointed verifiers. In Kilian [Kil01a], pages 388–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390388.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390388.pdf.

Chang:2001:CIU

[CL01b] Chin-Chen Chang and Iuon-Chang Lin. Cryptanalysis of the improved user efficient blind signatures. *Lecture Notes in Computer Science*, 2229:42–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290042.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290042.pdf.

Camenisch:2002:DAA

[CL02a] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Yung [Yun02a], pages 61–76. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Cao:2002:TKE

[CL02b] Zhen Fu Cao and Ji Guo Li. A threshold key escrow scheme based on ElGamal public key cryptosystem. *Chinese Journal of Computers = Chi suan chi hsueh pao*, 25(4):346–350, 2002. CODEN JIXUDT. ISSN 0254-4164.

Crowley:2002:BLS

[CL02c] Paul Crowley and Stefan Lucks. Bias in the LEVIATHAN stream cipher. *Lecture Notes in Computer Science*, 2355: 211–??, 2002. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550211.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550211.pdf.

Camenisch:2004:SSA

[CL04a] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Franklin [Fra04], pages 56–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Chang:2004:CGS

[CL04b] Chin-Chen Chang and Yeu-Pong Lai. A convertible group signature scheme. *Operating Systems Review*, 38(4):58–65, October 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chang:2004:IDM

[CL04c] Chin-Chen Chang and Iuon-Chang Lin. An improvement of delegated multisignature scheme with document decomposition. *Operating Systems Review*, 38(4):52–57, October 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chang:2004:RFB

[CL04d] Chin-Chen Chang and Iuon-Chang Lin. Remarks on fingerprint-based remote user authentication scheme using Smart Cards. *Operating Systems Review*, 38(4):91–96, October 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Camenisch:2005:FTO

[CL05] Jan Camenisch and Anna Lysyanskaya. A formal treatment of onion routing. In Shoup [Sho05a], pages 169–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Chandramouli:2007:ISS

[CL07] Ramaswamy Chandramouli and Philip Lee. Infrastructure standards for smart ID card deployment. *IEEE Security & Privacy*, 5(2):92–96, March/April 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Chang:2008:AWM

[CL08] Chin-Chen Chang and Pei-Yu Lin. Adaptive watermark mechanism for rightful ownership protection. *The Journal of Systems and Software*, 81(7):1118–1129, July 2008. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Chien:2009:EBL

[CL09] Hung-Yu Chien and Chi-Sung Laih. ECC-based lightweight authentication protocol with untraceability for low-cost RFID. *Journal of Parallel and Distributed Computing*, 69(10):848–853, October 2009. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Clark:2000:TNE

[Cla00a] David Clark. Technology news: Encryption advances to meet Internet challenges. *Computer*, 33(8):20–24, August 2000. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co2000/pdf/r8020.pdf.

Clark:2000:LNC

[Cla00b] Julie Clark. Looking for new contactless points: Hong Kong's Octopus smart card could get a lot smarter, but it will have to pick its way carefully through regulations and competition from other quarters first. *ITS international*, 6(2):77–78, March/April 2000.

Chen:2008:RCE

[CLC08] Tzung-Her Chen, Wei-Bin Lee, and Hsing-Bai Chen. A round- and computation-efficient three-party authenticated key exchange protocol. *The Journal of Systems and Software*, 81(9):1581–1590, September 2008. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Chang:2001:ASM

[CLK01a] Kyung-Ah Chang, Byung-Rae Lee, and Tai-Yun Kim. Authentication service model supporting multiple domains in distributed computing. *Lecture Notes in Computer Science*, 2073:413–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2073/20730413.htm; http://link.springer-ny.com/link/service/series/

0558/papers/2073/20730413.pdf.

Chang:2001:FAM

[CLK01b] Kyung-Ah Chang, Byung-Rae Lee, and Tai-Yun Kim. Flexible authentication with multiple domains of electronic commerce. *Lecture Notes in Computer Science*, 2115:176–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2115/21150176.htm; http://link.springer-ny.com/link/service/series/0558/papers/2115/21150176.pdf.

Cho:2004:GKR

[CLK04] Taenam Cho, Sang-Ho Lee, and Won Kim. A group key recovery mechanism based on logical key hierarchy. *Journal of Computer Security*, 12(5):711–736, ???? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cheon:2000:NBC

[CLLL00] Dong Hyeon Cheon, Sang Jin Lee, Jong In Lim, and Sung Jae Lee. New block cipher DONUT using pairwise perfect decorrelation. *Lecture Notes in Computer Science*, 1977: 262–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1977/19770262.htm; http://link.springer-ny.com/link/service/series/0558/papers/1977/19770262.pdf.

Canetti:2002:UCT

[CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. In ACM [ACM02], pages 494–503. ISBN 1-58113-495-9. LCCN QA75.5 .A22 2002. ACM order number 508020.

Cormen:2001:IA

[CLR01] Thomas H. Cormen, Charles E. (Eric) Leiserson, and Ronald L. Rivest. *Introduction to Algorithms*. MIT Press, Cambridge, MA, USA, second edition, 2001. ISBN 0-262-53196-8 (paperback), 0-262-03293-7 (hardcover), 0-07-013151-1 (McGraw-Hill), 0-07-297054-5 (McGraw-Hill with CD-ROM). xxi + 1180 pp. LCCN QA76.6 .I5858 2001.

Chen:2009:AKD

[CLR09] Bee-Chung Chen, Kristen Lefevre, and Raghu Ramakrishnan. Adversarial-knowledge dimensions in data privacy. *VLDB Journal: Very Large Data Bases*, 18(2):429–467, April 2009. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Chang:2007:SIH

[CLT07] Chin-Chen Chang, Chih-Yang Lin, and Chun-Sen Tseng. Secret image hiding and sharing based on the (t, n)-threshold. *Fundamenta Informaticae*, 76(4): 399–411, December 2007. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Clulow:2003:SP

[Clu03] Jolyon Clulow. On the security of PKCS #11. In Walter et al. [WKP03], pages 411–425. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240`.

Czumaj:2002:PTA

[CLZ02] Artur Czumaj, Andrzej Lingas, and Hairong Zhao. Polynomial-time approximation schemes for the Euclidean survivable network design problem. *Lecture Notes in Computer Science*, 2380:973–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2380/23800973.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2380/23800973.pdf`.

Camenisch:2000:CSS

[CM00] Jan Camenisch and Markus Michels. Confirmer signature schemes secure against adaptive adversaries (extended abstract). *Lecture Notes in Computer Science*, 1807:243–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070243.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1807/18070243.pdf`.

Cox:2002:FYE

[CM02] Ingemar J. Cox and Matt L. Miller. The first 50 years of electronic watermarking. *EURASIP Journal on Applied Signal Processing*, 2(1):126–132, January 2002. ISSN

1110-8657. URL http://delivery.acm.org/10.1145/1290000/1283114/p126-cox.pdf.

Courtois:2003:AAS

[CM03] Nicolas T. Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. *Lecture Notes in Computer Science*, 2656: 345–359, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_21.pdf.

Chevallier-Mames:2005:ECB

[CM05a] Benoît Chevallier-Mames. An efficient CDH-based signature scheme with a tight security reduction. In Shoup [Sho05a], pages 511–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Cojocaru:2005:ISM

[CM05b] Alina Cojocaru and Maruti Ram Murty. *An introduction to sieve methods and their applications*. London Mathematical Society student texts. Cambridge University Press, Cambridge, UK, 2005. ISBN 0-521-84816-4 (hardcover), 0-521-61275-6 (paperback). ???? pp. LCCN ????

Cox:2002:DW

[CMB02] Ingemar J. Cox, Matthew L. Miller, and Jeffrey A. Bloom. *Digital watermarking*. Morgan Kaufmann series in multimedia information and systems. Morgan Kaufmann Publishers, San Francisco, CA, USA, 2002. ISBN 1-55860-714-5. xxv + 542 pp. LCCN QA76.9.A25 C69 2002.

Crawford:2005:FBS

[CMB+05] Diane Crawford, Marius Matioc, Steven M. Bellovin, Richard Hubert, Andrew D. Wolfe, Jr., David Foulser, and Andrew R. Kilner. Forum: To block spam, demand sender authentication; not revolutionary (thank goodness); how to know the known from the unknowns; user first in user-centered design. *Communications of the Association for Computing Machinery*, 48(3):11–13, March 2005. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Cox:2008:DWS

[CMB+08] I. J. (Ingemar J.) Cox,

Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker. *Digital Watermarking and Steganography*. The Morgan Kaufmann series in multimedia information and systems; The Morgan Kaufmann series in computer security. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, second edition, 2008. ISBN 0-12-372585-2 (casebound). xxviii + 593 pp. LCCN QA76.9.A25 C68 2008. URL http://www.loc.gov/catdir/enhancements/fy0808/2007040595-d.html; http://www.loc.gov/catdir/toc/ecip081/2007040595.html.

Cremers:2006:ISE

[CMdV06] C. J. F. Cremers, S. Mauw, and E. P. de Vink. Injective synchronisation: an extension of the authentication hierarchy. *Theoretical Computer Science*, 367(1–2):139–161, November 24, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Campo:2001:JFC

[CMG+01] Celeste Campo, Andrés Marm, Arturo García, Ignacio Díaz, Peter T. Breuer, Carlos Delgado, and Carlos García. JCCM: Flexible certificates for smartcards with Java card. *Lecture Notes in Computer Science*, 2140:34–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400034.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400034.pdf.

Chevallier-Mames:2003:FDS

[CMJP03] Benoît Chevallier-Mames, Marc Joye, and Pascal Paillierinst. Faster double-size modular multiplication from Euclidean multipliers. In Walter et al. [WKP03], pages 214–227. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Chao:2000:CHC

[CMKT00] Jinhui Chao, Kazuto Matsuo, Hiroto Kawashiro, and Shigeo Tsujii. Construction of hyperelliptic curves with CM and its application to cryptosystems. *Lecture Notes in Computer Sci-*

ence, 1976:259–273, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cid:2006:AAA

[CMR06] Carlos Cid, Sean Murphy, and Matthew Robshaw. *Algebraic Aspects of the Advanced Encryption Standard*, volume 310 of *Advances in Information Security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 0-387-24363-1. 125 pp. LCCN ???? URL `http://deposit.ddb.de/cgi-bin/dokserv?id=2739239&prov=M&dok\_var=1&dok\_ext=htm`.

Cho:2008:DNP

[CMS08] Young H. Cho and William H. Mangione-Smith. Deep network packet filter design for reconfigurable devices. *ACM Transactions on Embedded Computing Systems*, 7(2):21:1–21:??, February 2008. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Caputo:2009:DIT

[CMS09] Deanna Caputo, Marcus Maloof, and Gregory Stephens. Detecting insider theft of trade secrets. *IEEE Security & Privacy*, 7(6): 14–21, November/December 2009. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Crawford:2002:FEE

[CNB+02] Diane Crawford, Srinivas Nedunuri, Adrian Bowyer, Arnd Weber, Greg A. Woods, and Mark Adler. Forum: Embrace the engineering metaphor; credit for crypto's parallel development; enough PDF: Give me HTML. *Communications of the Association for Computing Machinery*, 45(8):11–14, August 2002. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Coron:2004:SSL

[CNK04] Jean-Sebastien Coron, David Naccache, and Paul Kocher. Statistics and secret leakage. *ACM Transactions on Embedded Computing Systems*, 3(3):492–508, August 2004. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Ciet:2003:PFI

[CNPQ03] M. Ciet, M. Neve, E. Peeters, and J.-J. Quisquater. Parallel FPGA implementation of RSA with residue number systems — can side-channel threats be avoided? In *MWSCAS '03. Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Sys-*

tems, volume 2, pages 806–810. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2003. CODEN ???? ISSN ????

Catalano:2002:HHL

[CNS02] Dario Catalano, Phong Q. Nguyen, and Jacques Stern. The hardness of Hensel lifting: The case of RSA and discrete logarithm. *Lecture Notes in Computer Science*, 2501:299–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2501/25010299.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010299.pdf`.

Correia:2006:CAB

[CNV06] Miguel Correia, Nuno Ferreira Neves, and Paulo Veríssimo. From consensus to atomic broadcast: Time-free Byzantine-resistant protocols without signatures. *The Computer Journal*, 49(1):82–96, January 2006. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/cgi/content/abstract/49/1/82; http://comjnl.oxfordjournals.org/cgi/content/full/49/1/82; http://comjnl.oxfordjournals.org/cgi/reprint/49/1/82`.

Cetin:2009:NSA

[CO09a] Ozdemir Cetin and A. Turan Ozcerit. A new steganography algorithm based on color histograms for data embedding into raw video streams. *Computers & Security*, 28(7):670–682, October 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S016740480900042X`.

Czernik:2009:CRN

[CO09b] Pawel Czernik and Jakub Olszyna. Cryptographic random number generators for low-power distributed measurement system. *Proceedings of the SPIE — The International Society for Optical Engineering*, 7502 (1):75022A, 2009. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/7502/75022A/1`. Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2009.

Cobb:2004:CD

[Cob04] Chey Cobb. *Cryptography For Dummies*. For dummies. John Wiley and Sons, Inc., New York, NY, USA, 2004. ISBN 0-7645-4188-9. xx + 304 pp. LCCN TK5102.94 .C62 2004. US$24.99. URL http://www.loc.gov/catdir/bios/wiley046/2003105686.html; http://www.loc.gov/catdir/description/wiley039/2003105686.html; http://www.loc.gov/catdir/toc/wiley041/2003105686.html.

Cochran:2001:NVS

[Coc01a] Shannon Cochran. News and views: Scientists seek immersive reality; USENIX names lifetime achievement recipients [the GNU Project and the Kerberos network authentication system]; robots need programmers; evangelizing the Semantic Web; get your supercomputer software free; Usenet creator Jim Ellis dies; DARPA funds FreeBSD security initiative. *Dr. Dobb's Journal of Software Tools*, 26(9): 18, September 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Cocks:2001:IBE

[Coc01b] Clifford Cocks. An identity based encryption scheme based on quadratic residues. *Lecture Notes in Computer Science*, 2260:360–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600360.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600360.pdf.

Cochran:2002:NVSb

[Coc02a] Shannon Cochran. News and views: School of Adaptive Computer Training; it seems like yesterday… [10th anniversary of the first Web site]; double-gate transistor breakthrough; 802.11g Standard proposed; 30th anniversary of the [Intel] 4004; DeCSS legal decisions. *Dr. Dobb's Journal of Software Tools*, 27 (2):18, February 2002. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Cochran:2002:NVW

[Coc02b] Shannon Cochran. News and views: WaSP [Web Standards Project] buzzes off; Eclipse Project on the horizon; semiconductor roadmap: Ramping up, scaling down; AES [Advanced Encryption Standard]: Its finally official; SMS [Short Message Service] shines on; Berners-Lee awarded Japan Prize. *Dr. Dobb's Journal of Software Tools*, 27(3):14, March 2002. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Cochran:2003:NVC

[Coc03] Shannon Cochran. News and views: Cryptographers [Ronald Rivest, Adi Shamir, and Leonard Adleman] receive Turing Award; computer-science pioneer [John G. "Jack" Herriot] passes away; programming quantum computers; the demography of the Internet. *Dr. Dobb's Journal of Software Tools*, 28(7):14, July 2003. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/`.

Cohen:2003:FOV

[Coh03] Ernie Cohen. First-order verification of cryptographic protocols. *Journal of Computer Security*, 11(2):189–216, ???? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cole:2003:HPS

[Col03] Eric Cole. *Hiding in Plain Sight: Steganography and the Art of Covert Communication*. John Wiley and Sons, Inc., New York, NY, USA, 2003. ISBN 0-471-44449-9. xviii + 335 pp. LCCN QA76.9.A25 C598 2003. US$35.00.

Constantinou:2000:CSC

[Con00] Toulla Constantinou. Chicago smart: Chicago Transit Authority (CTS) joins "smart card" revolution. *Mass transit*, 26(7):52–53, December 2000.

Convery:2004:NSA

[Con04] Sean Convery. *Network security architectures*. Networking technology series. Cisco Press, Indianapolis, IN, USA, 2004. ISBN 1-58705-115-X. xxxix + 739 pp. LCCN TK5105.59 .C5793 2004. Duplicate ISBN with [TCR03].

Conti:2009:GSH

[Con09] Greg Conti. *Googling security: how much does Google know about you?* Addison-Wesley, Reading, MA, USA, 2009. ISBN 0-321-51866-7 (paperback). xxi + 332 pp. LCCN QA76.9.A25 C6678 2009. URL `http://www.loc.gov/catdir/toc/ecip0824/2008032687.html`.

Cook:2002:REJ

[Coo02] Jonathan J. Cook. Reverse execution of Java bytecode. *The Computer Journal*, 45 (6):608–619, ???? 2002. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_06/450608.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_06/pdf/450608.pdf`.

Coppersmith:2000:C

[Cop00] D. Coppersmith. Cryptography. *IBM Journal of Research and Development*, 44(1/2):246–250, January/March 2000. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL http://www.research.ibm.com/journal/rd/441/coppersmith.pdf. Special issue: reprints on Evolution of information technology 1957–1999.

Copeland:2004:COO

[Cop04a] B. Jack Copeland. Colossus: Its origins and originators. *IEEE Annals of the History of Computing*, 26(4):38–45, October/December 2004. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL http://csdl.computer.org/dl/mags/an/2004/04/a4038.htm; http://csdl.computer.org/dl/mags/an/2004/04/a4038.pdf.

Copeland:2004:ETS

[Cop04b] B. Jack Copeland, editor. *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life, plus The Secrets of Enigma*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2004. ISBN 0-19-825079-7 (hardcover), 0-19-825080-0 (paperback). viii + 613 pp. LCCN QA29.T8 E77 2004. URL ftp://uiarchive.cso.uiuc.edu/pub/etext/gutenberg/; http://www.loc.gov/catdir/toc/fy053/2004275594.html.

Copeland:2005:CSB

[Cop05] B. Jack Copeland, editor. *Colossus: the secrets of Bletchley Park's codebreaking computers*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2005. ISBN 0-19-284055-X. 344 (est.) pp. LCCN D810.C88 C66 2006.

Copeland:2006:CSB

[Cop06] B. Jack Copeland, editor. *Colossus: the secrets of Bletchley Park's codebreaking computers*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2006. ISBN 0-19-284055-X (hardcover), 0-19-957814-1 (paperback). xvi + 462 + 16 pp. LCCN D810.C88 C66 2006. URL http://www.colossus-computer.com/.

Copeland:2010:CSB

[Cop10] B. Jack Copeland, editor. *Colossus: the secrets of Bletchley Park's codebreaking computers*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2010. ISBN 0-19-284055-X (hardcover), 0-19-957814-1 (paperback). xvi + 462 + 16 pp. LCCN D810.C88 C66 2010. URL http://www.colossus-computer.com/.

Corella:2000:FIT

[Cor00a] Francisco Corella. A fast implementation of DES and Triple-DES on PA-RISC 2.0. In USENIX [USE00b], page ?? ISBN 1-880446-15-4. LCCN QA76.76.S95 W67 2000. URL http://www.usenix.org/publications/library/proceedings/osdi2000/wiess2000/corella.html.

Coron:2000:ESF

[Cor00b] Jean-Sébastien Coron. On the exact security of full domain hash. In Bellare [Bel00], pages 229–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800229.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800229.pdf.

Coron:2002:SPP

[Cor02] Jean-Sébastien Coron. Security proof for partial-domain hash signature schemes. In Yung [Yun02a], pages 613–626. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420613.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420613.pdf.

Coron:2006:WC

[Cor06] J.-S. Coron. What is cryptography? *IEEE Security & Privacy*, 4(1):70–73, January/February 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://ieeexplore.ieee.org/iel5/8013/33481/01588831.pdf; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=33481&arnumber=1588831.

Cosgrave:2000:NTC

[Cos00] John Cosgrave. Number theory and cryptography (using Maple). In *Coding theory and cryptography (Annapolis, MD, 1998)*, pages 124–143. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000.

Costlow:2003:BIM

[Cos03] Terry Costlow. In brief: Intelligent mail idea raising opponents' ire. *IEEE Distributed Systems Online*, 4(9), 2003. CODEN ???? ISSN 1541-4922 (print), 1558-1683 (electronic). URL http://

dsonline.computer.org/0309/d/brief.htm.

Courtois:2001:EZK

[Cou01] Nicolas T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. *Lecture Notes in Computer Science*, 2248: 402–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480402.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480402.pdf.

Courtois:2003:FAA

[Cou03] Nicolas T. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In Boneh [Bon03], pages 176–194. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Courtois:2004:FSB

[Cou04] Nicolas T. Courtois. Feistel schemes and bi-linear cryptanalysis: (extended abstract). In Franklin [Fra04], pages 23–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Courtois:2002:CBC

[CP02] Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. *Lecture Notes in Computer Science*, 2501: 267–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://eprint.iacr.org/2002/044/; http://link.springer.de/link/service/series/0558/bibs/2501/25010267.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010267.pdf.

Courtois:2003:AXA

[CP03] Nicolas T. Courtois and Jacques Patarin. About the XL algorithm over $GF(2)$. In Joye [Joy03b], pages 141–157. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Chatzikokolakis:2007:FAP

[CP07] Konstantinos Chatzikokolakis and Catuscia Palamidessi. A framework for analyzing probabilistic protocols and its application to the Partial Secrets Exchange. *Theoretical Computer Science*, 389(3):512–527, December 15, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Cimato:2006:PVC

[CPD06] S. Cimato, R. De Prisco, and A. De Santis. Probabilistic visual cryptography schemes. *The Computer Journal*, 49(1):97–107, January 2006. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/49/1/97; http://comjnl.oxfordjournals.org/cgi/content/full/49/1/97; http://comjnl.oxfordjournals.org/cgi/reprint/49/1/97.

Chow:2004:UDL

[CPG+04] Jim Chow, Ben Pfaff, Tal Garfinkel, Kevin Christopher, and Mendel Rosenblum. Understanding data lifetime via whole system simulation. In ????, editor, *USENIX Security Symposium*, page ?? USENIX, Berkeley, CA, USA, 2004. ISBN ???? LCCN ???? URL ????.

Chen:2004:SEP

[CPhX04] Ling Chen, Yi Pan, and Xiao hua Xu. Scalable and efficient parallel algorithms for Euclidean distance transform on the LARPBS model. *IEEE Transactions on Parallel and Distributed Systems*, 15(11):975–982, November 2004. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://csdl.computer.org/comp/trans/td/2004/11/l0975abs.htm; http://csdl.computer.org/dl/trans/td/2004/11/l0975.htm; http://csdl.computer.org/dl/trans/td/2004/11/l0975.pdf.

Catalano:2004:IIP

[CPP04] Dario Catalano, David Pointcheval, and Thomas Pornin. IPAKE: Isomorphisms for Password-Based

Authenticated Key Exchange. In Franklin [Fra04], pages 477–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Canetti:2007:CSH

[CPS07] R. Canetti, R. Pass, and A. Shelat. Cryptography from sunspots: How to use an imperfect reference string. In IEEE [IEE07], pages 249–259. ISBN 0-7695-3010-9. ISSN 0272-5428. LCCN QA76 .S974 2007. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4389466. IEEE Computer Society order number P3010.

Ciet:2001:SFC

[CQS01] M. Ciet, J.-J. Quisquater, and F. Sica. A secure family of composite finite fields suitable for fast implementation of elliptic curve cryptography. *Lecture Notes in Computer Science*, 2247: 108–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470108.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470108.pdf.

Canetti:2003:UCJ

[CR03] Ran Canetti and Tal Rabin. Universal composition with joint state. In Boneh [Bon03], pages 265–281. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Cramer:2005:ACE

[Cra05a] Ronald Cramer, editor. *Advances in cryptology: EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005, proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-

25910-4 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3494; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b136415.

Crampton:2005:UDR

[Cra05b] Jason Crampton. Understanding and developing role-based administrative models. In Meadows and Syverson [MS05b], pages 158–167. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Crenshaw:2000:SPK

[Cre00] Scott Crenshaw. Speedy public key cryptography system. *Network Security*, 2000(3):6, March 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800030130.

Crowley:2001:MFL

[Cro01] Paul Crowley. Mercy: a fast large block cipher for disk sector encryption. *Lecture Notes in Computer Science*, 1978:49–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780049.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780049.pdf.

Chhabra:2009:MSP

[CRSP09] Siddhartha Chhabra, Brian Rogers, Yan Solihin, and Milos Prvulovic. Making secure processors OS- and performance-friendly. *ACM Transactions on Architecture and Code Optimization*, 5(4):16:1–16:??, March 2009. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

CRI:2000:DPA

[Cry00] Cryptography Research, Inc. Differential power analysis. Web page., 2000. URL http://www.cryptography.com/dpa/index.html.

Cramer:2000:SSB

[CS00] Ronald Cramer and Victor Shoup. Signature schemes based on the strong RSA assumption. *ACM Transactions on Information and System Security*, 3(3):161–185, August 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cramer:2002:UHP

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. *Lecture Notes in Computer Science*, 2332: 45–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320045.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320045.pdf.

Camenisch:2003:PVE

[CS03a] Jan Camenisch and Victor Shoup. Practical verifiable encryption and decryption of discrete logarithms. In Boneh [Bon03], pages 126–144. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Cramer:2003:DAP

[CS03b] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, February 2003. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/40377.

Crepeau:2003:SBR

[CS03c] Claude Crépeau and Alain Slakmon. Simple backdoors for RSA key generation. In Joye [Joy03b], pages 403–416. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Carrier:2004:STP

[CS04] Brian Carrier and Clay Shields. The session token protocol for forensics and traceback. *ACM Transactions on Information and System Security*, 7(3):333–362, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Collberg:2005:SWF

[CS05a] Christian Collberg and Tapas Ranjan Sahoo. Software watermarking in the frequency domain: Implementation, analysis, and attacks. *Journal of Computer Security*, 13(5):721–755, ???? 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Contini:2005:SAA

[CS05b] Scott Contini and Igor E. Shparlinski. On Stern's attack against secret truncated linear congruential generators. *Lecture Notes in Computer Science*, 3574: 180–206, 2005. CODEN LNCSD9. ISBN 3-540-26547-3. ISSN 0302-9743 (print), 1611-3349 (electronic). Information Security and Privacy 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4–6, 2005. Proceedings.

Cvejic:2005:IRL

[CS05c] N. Cvejic and T. Seppänen. Increasing robustness of LSB audio steganography by reduced distortion LSB coding. *J.UCS: Journal of Universal Computer Science*, 11(1):56–65, January 28, 2005. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_11_1/increasing_robustness_of_lsb.

Capaldi:2007:ADI

[CS07a] Nicholas Capaldi and Miles Smit. *The art of deception: an introduction to critical thinking*. Prometheus Books, Amherst, NY, USA, 2007. ISBN 1-59102-532-X. 277 pp. LCCN BC177 .C345 2007. URL http://www.loc.gov/catdir/toc/ecip078/2007001612.html.

Chakrabarti:2007:PBA

[CS07b] Saikat Chakrabarti and Mukesh Singhal. Password-based authentication: Preventing dictionary attacks. *Computer*, 40(6):68–74, June 2007. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Chatterjee:2007:CSC

[CS07c] S. Chatterjee and P. Sarkar. Constant size ciphertext HIBE in the augmented selective-ID model and its extensions. *J.UCS: Journal of Universal Computer Science*, 13(10):1367–1395, ???? 2007. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_13_10/constant_size_ciphertext_hibe.

Casey:2008:IFD

[CS08a] Eoghan Casey and Gerasimos J. Stellatos. The impact of full disk encryption on digital forensics. *Operating Systems Review*, 42(3): 93–98, April 2008. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chang:2008:DAP

[CS08b] Katharine Chang and Kang G. Shin. Distributed Authentication of Program Integrity Verification in Wireless Sensor Networks. *ACM Transactions on Information and System Security*, 11(3):14:1–14:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cusick:2009:CBF

[CS09] Thomas W. Cusick and Pantelimon Stănică. *Cryptographic Boolean functions and applications*. Elsevier Academic Press, Amsterdam, The Netherlands, 2009. ISBN 0-12-374890-9 (hardcover). xii + 232 pp. LCCN QA10.3 .C87 2009.

Czeskis:2008:DED

[CSK+08] Alexei Czeskis, David J. St. Hilaire, Karl Koscher, Steven D. Gribble, Tadayoshi Kohno, and Bruce Schneier. Defeating encrypted and deniable file systems: Truecrypt V5.1a and the case of the tattling OS and applications. In ????, editor, *Proceedings of the 3rd Conference on Hot Topics in Security, 2008*, page ?? ????, ????, 2008. ISBN ???? LCCN ???? URL ????.

Cai:2007:CSM

[CSV07] Hongxu Cai, Zhong Shao, and Alexander Vaynberg. Certified self-modifying code. *ACM SIGPLAN Notices*, 42 (6):66–77, June 2007. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Crandall:2005:DUV

[CSW05] Jedidiah R. Crandall, Zhendong Su, and S. Felix Wu. On deriving unknown vulnerabilities from zero-day polymorphic and metamorphic worm exploits. In Meadows and Syverson [MS05b], pages 235–248. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Chen:2008:CCS

[CSW+08] L. Chen, W. Susilo, H. Wang, D. S. Wong, E. Dawson, X. Lai, M. Mambo, A. Miyaji, Y. Mu, D. Pointcheval, B. Preneel, and N. Smart. Cryptography in computer system security. *J.UCS: Journal of Universal Computer Science*, 14(3):314–317, ???? 2008. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_14; http://www.jucs.org/jucs_14_3#

; http://www.jucs.org/jucs_14_3/cryptography_in_computer_system.

Chung:2009:ISA

[CSY09] Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors. *Information Security Applications: 9th International Workshop, WISA 2008, Jeju Island, Korea, September 23–25, 2008, Revised Selected Papers*, volume 5379 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. CODEN LNCSD9. ISBN 3-642-00305-2 (print), 3-642-00306-0 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/content/978-3-642-00306-6.

Collberg:2002:WTP

[CT02] C. S. Collberg and C. Thomborson. Watermarking, tamper-proofing, and obfuscation — tools for software protection. *IEEE Transactions on Software Engineering*, 28(8):735–746, August 2002. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1027797.

Coron:2003:NAS

[CT03] Jean-Sébastien Coron and Alexei Tchulkine. A new algorithm for switching from arithmetic to Boolean masking. In Walter et al. [WKP03], pages 89–97. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Chen:2008:BUK

[CT08a] L. Chen and Q. Tang. Bilateral unknown key-share attacks in key agreement protocols. *J.UCS: Journal of Universal Computer Science*, 14(3):416–440, ???? 2008. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_14_3/bilateral_unknown_key_share.

Chu:2008:EOT

[CT08b] C.-K. Chu and W.-G. Tzeng. Efficient k-out-of-n oblivious transfer schemes. *J.UCS: Journal of Universal Computer Science*, 14 (3):397–415, ???? 2008.

CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_14_3/efficient_k_out_of.

Chou:2009:ATI

[CT09] Chang-Min Chou and Din-Chang Tseng. Affine-transformation-invariant public fragile watermarking for 3D model authentication. *IEEE Computer Graphics and Applications*, 29(2): 72–79, March/April 2009. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic).

Crawford:2001:FPV

[CTBA+01] Diane Crawford, Thomas Tiahrt, Moti Ben-Ari, Matt West, Hans A. von Spakovsky, and Deborah Phillips. Forum: Participatory vs. representative democracy; why store everything?; Emulex hoax; correction. *Communications of the Association for Computing Machinery*, 44(4):13–15, April 2001. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/2001-44-4/p13-crawford/. See [Sch00c, PvS01].

Chiang:2008:CPB

[CTH08] Yung-Kuei Chiang, Piyu Tsai, and Feng-Long Huang. Codebook partition based steganography without member restriction. *Fundamenta Informaticae*, 82(1–2):15–27, July 2008. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Chang:2004:ASS

[CTL04] Chin-Chen Chang, Piyu Tsai, and Min-Hui Lin. An adaptive steganographic scheme for color images. *Fundamenta Informaticae*, 62(3–4):275–289, March 2004. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Cheung:2001:TPS

[CTLL01] O. Y. H. Cheung, K. H. Tsoi, P. H. W. Leong, and M. P. Leong. Tradeoffs in parallel and serial implementations of the international data encryption algorithm IDEA. *Lecture Notes in Computer Science*, 2162:333–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620333.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620333.pdf.

Collberg:2007:DGB

[CTT07] Christian S. Collberg, Clark Thomborson, and Gregg M.

Townsend. Dynamic graph-based software fingerprinting. *ACM Transactions on Programming Languages and Systems*, 29(6):35:1–35:67, October 2007. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).

Chen:2009:FCV

[CTY09] Tzung-Her Chen, Kai-Hsiang Tsao, and Yan-Ting Yang. Friendly color visual secret sharing by random grids. *Fundamenta Informaticae*, 96(1–2):61–70, January 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Cheng:2001:NPT

[CU01] Qi Cheng and Shigenori Uchiyama. Nonuniform polynomial time algorithm to solve decisional Diffie–Hellman problem in finite fields under conjecture. *Lecture Notes in Computer Science*, 2271: 290–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710290.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710290.pdf`.

Curtin:2005:BFC

[Cur05] Matt Curtin. *Brute force: cracking the Data Encryption Standard*. Copernicus (a division of Springer-Verlag New York, Inc.), 175 Fifth Avenue, New York, NY 10010, USA, 2005. ISBN 0-387-20109-2. x + 291 pp. LCCN QA76.9.A25 C873 2005.

Chaitanya:2008:QQM

[CUS08] Shiva Chaitanya, Bhuvan Urgaonkar, and Anand Sivasubramaniam. QDSL: a queuing model for systems with differential service levels. *ACM SIGMETRICS Performance Evaluation Review*, 36(1):289–300, June 2008. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Canteaut:2002:DCH

[CV02] Anne Canteaut and Marion Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. *Lecture Notes in Computer Science*, 2332:518–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320518.htm; http://link.springer-ny.com/link/service/series/`

0558/papers/2332/23320518.pdf.

Cary:2003:MAC

[CV03] Matthew Cary and Ramarathnam Venkatesan. A message authentication code based on unimodular matrix groups. In Boneh [Bon03], pages 500–512. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Canteaut:2004:PCI

[CV04] Anne Canteaut and Kapaleeswaran Viswanathan, editors. *Progress in cryptology: INDOCRYPT 2004: 5th International Conference on Cryptology in India, Chennai, India, December 20–22, 2004: Proceedings*, volume 3348 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-24130-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I5535 2004. URL http://springerlink.metapress.com/openurl.asp?genre=issue&issn=0302-9743&volume=3348; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3348; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b104579.

Castro:2005:NRG

[CV05] Julio César Hernández Castro and Pedro Isasi Viñuela. New results on the genetic cryptanalysis of TEA and reduced-round versions of XTEA. *New Generation Computing*, 23(3):233–243, 2005. CODEN NGCOE5. ISSN 0288-3635 (print), 1882-7055 (electronic). URL http://www.springerlink.com/content/e018uh040400kh87/.

Canda:2001:SBC

[ČvTMH01] Valér Čanda, Tran van Trung, Spyros Magliveras, and Tamás Horváth. Symmetric block ciphers based on group bases. *Lecture Notes in Computer Science*, 2012:89–105, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120089.htm; http://link.springer-

ny.com/link/service/series/0558/papers/2012/20120089.pdf.

Chang:2002:ATI

[CW02] Fu-Chi Chang and Chia-Jiu Wang. Architectural tradeoff in implementing RSA processors. *ACM SIGARCH Computer Architecture News*, 30(1):5–11, March 2002. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Chess:2007:SPS

[CW07] Brian Chess and Jacob West. *Secure programming with static analysis*. Addison-Wesley software security series. Addison-Wesley, Reading, MA, USA, 2007. ISBN 0-321-42477-8 (paperback). xxix + 587 pp. LCCN QA76.9.A25 C443 2007. URL http://www.loc.gov/catdir/toc/ecip0713/2007010226.html.

Cheng:2009:NAS

[CW09] Yu-Ming Cheng and Chung-Ming Wang. A novel approach to steganography in high-dynamic-range images. *IEEE MultiMedia*, 16(3):70–80, July/September 2009. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Chang:2000:ELD

[CWH00] Yuh-Shihng Chang, Tzong-Chen Wu, and Shih-Chan Huang. ElGamal-like digital signature and multisignature schemes using self-certified public keys. *The Journal of Systems and Software*, 50(2):99–105, February 15, 2000. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.elsevier.nl/gej-ng/10/29/11/49/27/26/article.pdf; http://www.elsevier.nl/gej-ng/10/29/11/49/27/abstract.html.

Chien:2001:CCW

[CWJT01] Hung-Yu Chien, Tzong-Chen Wu, Jinn-Ke Jan, and Yuh-Min Tseng. Cryptanalysis of Chang–Wu's group-oriented authentication and key exchange protocols. *Information Processing Letters*, 80(2):113–117, October 31, 2001. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.com/gej-ng/10/23/20/80/37/33/abstract.html.

Crosby:2009:OLR

[CWR09] Scott A. Crosby, Dan S. Wallach, and Rudolf H. Riedi. Opportunities and limits of remote timing attacks. *ACM Transactions* *on Information and System Security*, 12(3):17:1–17:??, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chien:2005:NRS

[CWY05] Hung-Yu Chien, Ren-Chiun Wang, and Chou-Chen Yang. Note on robust and simple authentication protocol. *The Computer Journal*, 48(1):27–29, January 2005. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_48/Issue_01/bxh061.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_48/Issue_01/pdf/bxh061.pdf.

Choie:2002:ICH

[CY02] Y. Choie and D. Yun. Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbf{F}_q$. *Lecture Notes in Computer Science*, 2384:190–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840190.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840190.pdf.

Chen:2005:ENB

[CY05] Yen-Cheng Chen and Lo-Yao Yeh. An efficient nonce-based authentication scheme with key agreement. *Applied Mathematics and Computation*, 169(2):982–994, October 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2008:EBD

[CY08] Mei-Chu Chang and Chui Zhi Yao. An explicit bound on double exponential sums related to Diffie–Hellman distributions. *SIAM Journal on Discrete Mathematics*, 22(1):348–359, ???? 2008. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Chang:2001:NSS

[CYH01] Chin-Chen Chang, Jyh-Chiang Yeh, and Ju-Yuan Hsiao. A novel scheme for securing image steganography. *Lecture Notes in Computer Science*, 2195:804–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950804.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950804.pdf.

Chang:2004:TSSb

[CYH04] Ting-Yi Chang, Chou-Chen Yang, and Min-Shiang Hwang. A threshold signature scheme for group communications without a shared distribution center. *Future Generation Computer Systems*, 20(6):1013–1021, August 2004. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Chang:2005:SAK

[CYH05] Ting-Yi Chang, Wei-Pang Yang, and Min-Shiang Hwang. Simple authenticated key agreement and protected password change protocol. *Computers and Mathematics with Applications*, 49(5–6):703–714, April/May 2005. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122105000842.

Chung:2007:SBW

[CYH+07] Kuo-Liang Chung, Wei-Ning Yang, Yong-Huai Huang, Shih-Tung Wu, and Yu-Chiao Hsu. On SVD-based watermarking algorithm. *Applied Mathematics and Computation*, 188 (1):54–57, May 1, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2005:CIA

[CYY05] Ting-Yi Chang, Chou-Chan Yang, and Ya-Wen Yang. Cryptanalysis of the improved authenticated key agreement protocol. *Applied Mathematics and Computation*, 171(2):771–774, December 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chen:2003:AEY

[CZ03] Ke-Fei Chen and Sheng Zhong. Attacks on the (enhanced) Yang–Shieh authentication. *Computers & Security*, 22(8):725–727, December 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803000129. See erratum [McK04].

Chadwick:2005:PKI

[CZ05] David Chadwick and Gansen Zhao, editors. *Public key infrastructure: Second European PKI Workshop: Research and Applications, EuroPKI 2005, Canterbury, UK, June 30–July 1, 2005: revised selected papers*, volume 3545 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-

28062-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E976 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3545.

Crawford:2001:FHC

[CZB+01] Diane Crawford, Mick Zraly, Hal Berghel, Ken Pugh, Mat H. West, Conrad Weisert, Terry Steyaert, and Richard Johnson. Forum: How can the Web advance Western democracies? who needs digital signatures; misinformation and the Emulex hoax; OOSCD not really so unified; go back to non-OOSD. *Communications of the Association for Computing Machinery*, 44(2):11–13, February 2001. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/2001-44-2/p11-crawford/. See [Sch00c].

Cheng:2005:RIC

[CZK05] Xiaorong Cheng, Huilan Zhao, and Jitian Kou. Research and improvement on computer intrusion detection technology based on immune principle. In Han et al. [HYZ05b], pages 167–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Dodis:2003:CAA

[DA03] Yevgeniy Dodis and Jee Hea An. Concealment and its applications to authenticated encryption. *Lecture Notes in Computer Science*, 2656:312–329, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_19.pdf.

Dale:2001:BSA

[Dal01] Richard Dale. Biometric security: It's all about identification and authentication. *Dr. Dobb's Journal of Software Tools*, 26(11):93–94, 96, November 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Damgaard:2000:ECZ

[Dam00] Ivan Damgård. Efficient concurrent zero-knowledge in the auxiliary string model. In ????, editor, *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, pages 418–430. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN ???? LCCN ???? URL ????.

Damaj:2007:PAD

[Dam07] Issam W. Damaj. Parallel algorithms development for programmable devices with application from cryptography. *International Journal of Parallel Programming*, 35(6):529–572, December 2007. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0885-7458&volume=35&issue=6&spage=529.

Danielyan:2001:AAE

[Dan01] Edgar Danielyan. AES: Advanced Encryption Standard is coming. *;login: the USENIX Association newsletter*, 26(1):??, February 2001. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/2001-02/pdfs/danielyan.pdf.

Danas:2002:CUS

[Dan02] George Danas. On a cryptosystem using simple continued fractions. *Math. Sci. Res. J.*, 6(3):168–173, 2002. ISSN 1537-5978.

Das:2008:BQC

[Das08] S. R. Das. Breaking quantum cryptography's 150-kilometer limit [update]. *IEEE Spectrum*, 45(9):15, September 2008. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Davis:2001:ISV

[Dav01a] Carlton R. Davis. *IPSec: Securing VPNs*. McGraw-Hill, New York, NY, USA, 2001. ISBN 0-07-212757-0. xix + 404 pp. LCCN TK5105.567 D38 200. US$49.99.

Davis:2001:DSA

[Dav01b] Don Davis. Defective Sign & Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML. In USENIX [USE01a], page ?? ISBN 1-880446-09-X. LCCN QA76.8.U65 U84 2001. URL http://www.usenix.org/publications/library/proceedings/usenix01/davis.html.

Davis:2001:DSE

[Dav01c] Don Davis. Defective sign-and-encrypt: Can you really trust S/MIME, PCKS#7, PGP, and XML? *Dr. Dobb's Journal of Software Tools*, 26(11):30, November 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Davis:2007:AAA

[Dav07] Adrian Davis. Authentication across the airwaves. *Network Security*, 2007(2):13–19, February 2007. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485807700193.

DeBrosse:2004:SBU

[DB04] Jim DeBrosse and Colin B. Burke. *The secret in Building 26: the untold story of America's ultra war against the U-boat Enigma codes.* Random House, New York, NY, USA, 2004. ISBN 0-375-50807-4, 1-58836-353-8, 0-375-75995-6. xxix + 272 pp. LCCN D810.C88 D43 2004. URL http://www.loc.gov/catdir/samples/random045/2003058494.html; http://www.randomhouse.com/catalog/display.pperl?isbn=9781588363534.

deBorde:2007:STF

[dB07] Duncan de Borde. Selecting a two-factor authentication system. *Network Security*, 2007(7):17–20, July 2007. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485807700661.

Desmedt:2001:ERD

[DBS01] Yvo Desmedt, Mike Burmester, and Jennifer Seberry. Equitability in retroactive data confiscation versus proactive key escrow. *Lecture Notes in Computer Science*, 1992:277–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920277.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920277.pdf.

Doyle:2006:SCK

[DBS+06] Barry Doyle, Stuart Bell, Alan F. Smeaton, Kealan McCusker, and Noel E. O'Connor. Security considerations and key negotiation techniques for power constrained sensor networks. *The Computer Journal*, 49(4):443–453, July 2006. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/49/4/443; http://comjnl.oxfordjournals.org/cgi/content/full/49/4/443; http://comjnl.oxfordjournals.org/cgi/reprint/49/4/443.

diVimercati:2005:CSE

[dCdVSG05] Sabrina de Capitani di Vimercati, Paul Syverson, and Dieter Gollmann, editors. *Computer security — ESORICS 2005: 10th European symposium on research in computer security, Milan, Italy, September 12–14, 2005: proceedings*, volume 3679 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-28963-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ????

DeBonis:2000:RVC

[DD00] Annalisa De Bonis and Alfredo De Santis. Randomness in visual cryptography. *Lecture Notes in Computer Science*, 1770: 626–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1770/17700626.htm; http://link.springer-ny.com/link/service/series/0558/papers/1770/17700626.pdf.

Dalkilic:2002:CPF

[DD02] Mehmet Emin Dalkiliç and Gökhan Dalkiliç. On the cryptographic patterns and frequencies in Turkish language. *Lecture Notes in Computer Science*, 2457: 144–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2457/24570144.htm; http://link.springer.de/link/service/series/0558/papers/2457/24570144.pdf.

DeBonis:2004:RSS

[DD04] Annalisa De Bonis and Alfredo De Santis. Randomness in secret sharing and visual cryptography schemes. *Theoretical Computer Science*, 314(3):351–374, April 10, 2004. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Diene:2006:DLE

[DDG+06] Adama Diene, Jintai Ding, Jason E. Gower, Timothy J. Hodges, and Zhijun Yin. Dimension of the linearization equations of the Matsumoto–Imai cryptosystems. In Ytrehus [Ytr06], pages 242–251. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Dolev:2000:NC

[DDN00] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, April 2000. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/29156.

Dolev:2003:NC

[DDN03] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM Review*, 45(4):727–

784, December 2003. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/42985`.

DeSantis:2001:RNI

[DDO+01] Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, and Amit Sahai. Robust non-interactive zero knowledge. In Kilian [Kil01a], pages 566–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390566.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2139/21390566.pdf`.

Dean:2006:IMB

[Dea06] Roger Dean. Identity management — back to the user. *Network Security*, 2006(12): 4–7, December 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485806704603`.

DeLooze:2007:PWS

[DeL07] Lori DeLooze. Providing Web service security in a federated environment. *IEEE Security & Privacy*, 5(1):73–75, January/February 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Desai:2000:ESS

[Des00a] Anand Desai. *Encryption schemes: security notions, designs and analyses*. Vita thesis (Ph.D.), University of California, San Diego, San Diego, CA, USA, 2000.

Desai:2000:NPC

[Des00b] Anand Desai. New paradigms for constructing symmetric encryption schemes secure against chosen-ciphertext attack. In Bellare [Bel00], pages 394–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800394.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1880/18800394.pdf`.

Desai:2000:SAN

[Des00c] Anand Desai. The security of all-or-nothing encryption: Protecting against exhaustive key search. In Bellare [Bel00], pages 359–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25

C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800359.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800359.pdf.

Desmedt:2002:PKC

[Des02] Yvo G. Desmedt, editor. *Public Key Cryptography—PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography Miami, FL, USA, January 6–8, 2003. Proceedings*, volume 2567 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-00324-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I567 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2567.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2567. Also available via the World Wide Web.

Dewson:2008:BSS

[Dew08] Robin Dewson. *Beginning SQL Server 2008 for developers: from novice to professional; [the quick and efficient path to proficiency in SQL Server 2008]*. The expert's voice in SQL Server. Apress, Berkeley, CA, USA, 2008. ISBN 1-59059-958-6. xxiv + 471 pp. LCCN ????

Dhem:2001:HSS

[DF01] Jean-François Dhem and Nathalie Feyt. Hardware and software symbiosis helps smart card evolution. *IEEE Micro*, 21(6):14–25, November/December 2001. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://dlib.computer.org/mi/books/mi2001/m6014abs.htm; http://dlib.computer.org/mi/books/mi2001/pdf/m6014.pdf.

Delgado:2007:SCD

[DF07] Oscar Delgado and Amparo Fúster. Stream cipher design for MANets. In Simos and Maroulis [SM07b], pages 965–968. ISBN 0-7354-0476-3 (set), 0-7354-0477-1 (vol. 1), 0-7354-0478-X (vol. 2). ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. LCCN Q183.9 .I524 2007. URL http://proceedings.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf& id=APCPCS000963000002000965000001& idtype=cvips.

Domingo-Ferrer:2000:SCR

[DFCW00] Josep Domingo-Ferrer, David Chan, and Anthony Watson, editors. *Smart card research and advanced applications: IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, September 20–22, 2000, Bristol, United Kingdom*, volume 52 of *IFIP*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2000. ISBN 0-7923-7953-5. LCCN TK7895.S62 I34 2000.

Durante:2000:CAC

[DFG00] Antonio Durante, Riccardo Focardi, and Roberto Gorrieri. A compiler for analyzing cryptographic protocols using noninterference. *ACM Transactions on Software Engineering and Methodology*, 9(4):488–528, October 2000. CODEN ATSMER. ISSN 1049-331X (print), 1557-7392 (electronic). URL `http://www.acm.org/pubs/articles/journals/tosem/2000-9-4/p488-durante/p488-durante.pdf; http://www.acm.org/pubs/citations/journals/tosem/2000-9-4/p488-durante/`.

Durante:2001:CWR

[DFG01] Antonio Durante, Riccardo Focardi, and Roberto Gorrieri. CVS at work: a report on new failures upon some cryptographic protocols. *Lecture Notes in Computer Science*, 2052: 287–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2052/20520287.htm; http://link.springer-ny.com/link/service/series/0558/papers/2052/20520287.pdf`.

DePalma:2004:CCS

[DFGH04] Paul De Palma, Charles Frank, Suzanne Gladfelter, and Joshua Holden. Cryptography and computer security for undergraduates. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 36(1):94–95, March 2004. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Domingo-Ferrer:2001:CDS

[DFH01] Josep Domingo-Ferrer and Pieter Hartel. Current directions in smart cards. *Computer Networks (Amsterdam, Netherlands: 1999)*, 36(4):377–379, July 16, 2001. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.elsevier.nl/gej-ng/10/15/22/61/28/25/abstract.html; http:`

//www.elsevier.nl/gej-ng/10/15/22/61/28/25/article.pdf.

Dodis:2003:IRP

[DFK+03] Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji, and Moti Yung. Intrusion-resilient public-key encryption. In Joye [Joy03b], pages 19–32. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

DeSantis:2004:CKA

[DFM04] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Cryptographic key assignment schemes for any access control policy. *Information Processing Letters*, 92(4):199–205, November 30, 2004. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Domingo-Ferrer:2006:SCR

[DFPS06] Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors. *Smart Card Research and Advanced Applications: 7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006, Tarragona, Spain, April 19–21, 2006. Proceedings*, volume 3928 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-33311-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3928.

Domingo-Ferrer:2007:ASC

[DFPST07] Josep Domingo-Ferrer, Joachim Posegga, Francesc Sebé, and Vicenç Torra. Advances in smart cards. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(9):2219–2222, June 20, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Damgaard:2004:ZKP

[DFS04] Ivan Damgård, Serge Fehr, and Louis Salvail. Zero-knowledge proofs and string commitments withstanding quantum attacks. In Franklin [Fra04], pages 254–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.

com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Damgard:2005:CBQ

[DFSS05] I. B. Damgard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In IEEE [IEE05a], pages 449–458. ISBN 0-7695-2468-0, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S979 2005. IEEE Computer Society order number P2468.

Damgaard:2008:CBQ

[DFSS08] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, ???? 2008. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Dalkilic:2000:ICA

[DG00] Mehmet E. Dalkilic and Cengiz Gungor. An interactive cryptanalysis algorithm for the Vigenère cipher. *Lecture Notes in Computer Science*, 1909: 341–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1909/19090341.htm; http://link.springer-ny.com/link/service/series/0558/papers/1909/19090341.pdf.

Debaert:2002:RRI

[DG02] Christophe Debaert and Henri Gilbert. The RIPEMD and RIPEMD improved variants of MD4 are not collision free. *Lecture Notes in Computer Science*, 2355: 52–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550052.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550052.pdf.

DiRaimondo:2003:PST

[DG03] Mario Di Raimondo and Rosario Gennaro. Provably secure threshold password-authenticated key exchange. *Lecture Notes in Computer Science*, 2656:507–523, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_32.pdf.

DiRaimondo:2005:NAD

[DG05] Mario Di Raimondo and

Rosario Gennaro. New approaches for deniable authentication. In Meadows and Syverson [MS05b], pages 112–121. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

DiRaimondo:2006:PST

[DG06] Mario Di Raimondo and Rosario Gennaro. Provably secure threshold password-authenticated key exchange. *Journal of Computer and System Sciences*, 72(6):978–1001, September 2006. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002200000600033X.

Dodis:2004:REK

[DGH+04] Yevgeniy Dodis, Rosario Gennaro, Johan Håstad, Hugo Krawczyk, and Tal Rabin. Randomness extraction and key derivation using the CBC, Cascade and HMAC modes. In Franklin [Fra04], pages 494–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Devanbu:2004:FAX

[DGK+04] Premkumar Devanbu, Michael Gertz, April Kwong, Charles Martel, Glen Nuckolls, and Stuart G. Stubblebine. Flexible authentication of XML documents. *Journal of Computer Security*, 12(6):841–864, ???? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Devanbu:2003:ADP

[DGMS03] Premkumar Devanbu, Michael Gertz, Charles Martel, and Stuart G. Stubblebine. Authentic data publication over the Internet. *Journal of Computer Security*, 11(3):291–314, ???? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dwork:2003:MBF

[DGN03] Cynthia Dwork, Andrew Goldberg, and Moni Naor. On memory-bound functions for fighting spam. In Boneh [Bon03], pages 426–444. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.

com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Dorrendorf:2007:CRNa

[DGP07a] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. Technical report 2007/419, Cryptology ePrint Archive, International Association for Cryptologic Research, San Jose, CA, USA, 2007. URL http://eprint.iacr.org/2007/419.

Dorrendorf:2007:CRNb

[DGP07b] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. In *CCS '07: Proceedings of the 14th ACM conference on computer and communications security*, page ???? ACM Press, New York, NY 10036, USA, 2007. ISBN 1-59593-703-X. LCCN ????

Dorrendorf:2009:CRN

[DGP09] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. *ACM Transactions on Information and System Security*, 13(1):10:1–10:32, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

denHartog:2008:TMC

[dH08] Jerry den Hartog. Towards mechanized correctness proofs for cryptographic algorithms: Axiomatization of a probabilistic Hoare style logic. *Science of Computer Programming*, 74(1–2):52–63, December 1, 2008. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic).

Dhem:2003:EMR

[Dhe03] Jean-François Dhem. Efficient modular reduction algorithm in and its application to “left to right” modular multiplication in. In Walter et al. [WKP03], pages 203–213. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Deng:2006:OOC

[DHL06] Yan-Xiang Deng, Chao-Jang Hwang, and Jiang-

Lung Liu. An object-oriented cryptosystem based on two-level reconfigurable computing architecture. *The Journal of Systems and Software*, 79(4):466–479, April 2006. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Daza:2007:CTM

[DHMR07] Vanesa Daza, Javier Herranz, Paz Morillo, and Carla Ràfols. Cryptographic techniques for mobile ad-hoc networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(18):4938–4950, December 19, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Dodis:2000:CSG

[DHR00] Yevgeniy Dodis, Shai Halevi, and Tal Rabin. A cryptographic solution to a game theoretic problem. In Bellare [Bel00], pages 112–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800112.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800112.pdf`.

DiCrescenzo:2001:SOS

[Di 01] Giovanni Di Crescenzo. Sharing one secret vs. sharing many secrets: Tight bounds for the max improvement ratio. *Lecture Notes in Computer Science*, 2136:292–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2136/21360292.htm; http://link.springer-ny.com/link/service/series/0558/papers/2136/21360292.pdf`.

DiCrescenzo:2003:SOS

[Di 03] Giovanni Di Crescenzo. Sharing one secret vs. sharing many secrets. *Theoretical Computer Science*, 295(1–3):123–140, February 24, 2003. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Damgaard:2005:CRM

[DI05] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. In Shoup [Sho05a], pages 378–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9

C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Dichtl:2003:HPO

[Dic03] Markus Dichtl. How to predict the output of a hardware random number generator. In Walter et al. [WKP03], pages 181–188. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Dierickx:2000:EGD

[Die00] Jürgen Dierickx. European guidelines for digital signatures. *Network Security*, 2000(3):3–4, March 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800030063.

Diffie:2001:UC

[Dif01] Whitfield Diffie. Ultimate cryptography. *Communications of the Association for Computing Machinery*, 44(3):84–86, March 2001. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/2001-44-3/p84-diffie/.

Dimitriadis:2007:IMC

[Dim07] Christos K. Dimitriadis. Improving mobile core network security with honeynets. *IEEE Security & Privacy*, 5(4):40–47, July/August 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Dimitrov:2008:DBN

[DIM08] Vassil Dimitrov, Laurent Imbert, and Pradeep K. Mishra. The double-base number system and its application to elliptic curve cryptography. *Mathematics of Computation*, 77(262):1075–1104, April 2008. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2008-77-262/S0025-5718-07-02048-0/home.html; http://www.ams.org/mcom/2008-77-262/S0025-5718-07-02048-0/S0025-5718-07-02048-0.dvi; http://www.ams.org/mcom/2008-77-262/S0025-5718-07-02048-0/S0025-

5718-07-02048-0.pdf; http://www.ams.org/mcom/2008-77-262/S0025-5718-07-02048-0/S0025-5718-07-02048-0.ps.

Ding:2001:OTB

[Din01] Yan Zong Ding. Oblivious transfer in the bounded storage model. In Kilian [Kil01a], pages 155–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390155.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390155.pdf.

Ding:2005:ECB

[Din05] Yan Zong Ding. Error correction in the bounded storage model. In Kilian [Kil05], pages 578–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Dedic:2005:ULB

[DIRR05] Nenad Dedić, Gene Itkis, Leonid Reyzin, and Scott Russell. Upper and lower bounds on black-box steganography: Extended abstract. In Kilian [Kil05], pages 227–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Dang:2002:EPT

[DIS02] Zhe Dang, Oscar H. Ibarra, and Zhi-Wei Sun. On the emptiness problem for two-way NFA with one reversal-bounded counter. *Lecture Notes in Computer Science*, 2518:103–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2518/25180103.htm; http://link.springer.de/link/service/series/0558/papers/2518/25180103.pdf.

Damgaard:2001:GSS

[DJ01] Ivan Damgård and Mads Jurik. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. *Lecture Notes in Computer Science*, 1992: 119–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920119.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920119.pdf.

Delaune:2006:DPS

[DJ06] Stéphanie Delaune and Florent Jacquemard. Decision procedures for the security of protocols with probabilistic encryption against offline dictionary attacks. *Journal of Automated Reasoning*, 36(1–2):85–124, January 2006. CODEN JAREEW. ISSN 0168-7433 (print), 1573-0670 (electronic). URL http://link.springer.com/article/10.1007/s10817-005-9017-7.

Donsez:2001:TMA

[DJLT01] Didier Donsez, Sébastien Jean, Sylvain Lecomte, and Olivier Thomas. Turning multi-applications smart cards services available from anywhere at anytime: a SOAP /MOM approach in the context of Java cards. *Lecture Notes in Computer Science*, 2140: 83–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400083.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400083.pdf.

Damgaard:2001:PTR

[DK01] Ivan Damgård and Maciej Koprowski. Practical threshold RSA signatures without a trusted dealer. *Lecture Notes in Computer Science*, 2045: 152–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450152.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450152.pdf.

Delfs:2002:ICP

[DK02] Hans Delfs and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. ISBN 3-642-87126-7 (e-book), 3-642-87128-3. ISSN 1619-

7100 (print), 2197-845X (electronic). xiv + 310 pp. LCCN QA76.9.A25. URL http://www.springerlink.com/content/978-3-642-87126-9.

Dodis:2005:CCS

[DK05] Yevgeniy Dodis and Jonathan Katz. Chosen-ciphertext security of multiple encryption. In Kilian [Kil05], pages 188–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Delfs:2007:ICP

[DK07] Hans Delfs and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*, volume 1 of *Information Security and Cryptography*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2007. ISBN 3-540-49243-7 (hardcover), 3-540-49244-5. ISSN 1619-7100 (print), 2197-845X (electronic). xvi + 367 pp. LCCN QA76.9A25 D44 2007; QA76.9.D35. URL http://www.springerlink.com/content/gm2886.

Dunkelman:2008:TIV

[DK08] Orr Dunkelman and Nathan Keller. Treatment of the initial value in Time-Memory-Data Tradeoff attacks on stream ciphers. *Information Processing Letters*, 107(5): 133–137, August 16, 2008. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Du:2005:BRS

[DKFX05] Xiaozhen Du, Weidong Kou, Kai Fan, and Yuxia Xiao. Breaking and repairing of a strong proxy signature scheme with proxy signer privacy protection. In Han et al. [HYZ05b], pages 100–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Daswani:2007:FSW

[DKK07] Neil Daswani, Christoph Kern, and Anita Kesavan. *Foundations of security: what every programmer needs to know*. The Expert's voice in security. Apress, Berkeley, CA, USA, 2007. ISBN 1-59059-784-2 (paperback). xxvii + 290 pp. LCCN QA76.76.P76 D37 2007.

Dhem:2000:PIT

[DKL+00a] Jean-François Dhem, François Koeune, Philippe-Alexandre Leroux, Patrick Mestr, Jean-Jacques Quisquater, and Jean-Louis Willems. A practical implementation of the timing attack. In ????, editor, *Smart Card Research and Applications*, volume 1820, pages 167–182. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN ???? LCCN ???? URL ????.

Ding:2000:SSC

[DKL00b] Cunsheng Ding, David R. Kohel, and San Ling. Secret-sharing with a class of ternary codes. *Theoretical Computer Science*, 246(1–2):285–298, September 6, 2000. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.nl/gej-ng/10/41/16/180/21/34/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/180/21/34/article.pdf.

Dodis:2009:CAI

[DKL09] Yevgeniy Dodis, Yael Tauman Kalai, and Shachar Lovett. On cryptography with auxiliary input. In ACM [ACM09], pages 621–630. ISBN 1-60558-613-7. LCCN QA75.5 .A22 2009.

Datta:2005:RBN

[DKMR05] Anupam Datta, Ralf Küsters, John C. Mitchell, and Ajith Ramanathan. On the relationships between notions of simulation-based security. In Kilian [Kil05], pages 476–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Delaune:2008:FAP

[DKS08] Stéphanie Delaune, Steve Kremer, and Graham Steel. Formal analysis of PKCS#11. In ????, editor, *IEEE Computer Security Foundations Symposium*, pages 331–344. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. ISBN ???? LCCN ???? URL ????.

Dittmann:2005:CMS

[DKU05] Jana Dittmann, Stefan Katzenbeisser, and Andreas Uhl, editors. *Communications and multimedia security: 9th IFIP TC-6 TC-11 International Conference, CMS 2005, Salzburg,* *Austria, September 19–21, 2005: proceedings*, volume 3677 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-28791-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ????

Dodis:2002:KIP

[DKXY02] Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung. Key-insulated public key cryptosystems. *Lecture Notes in Computer Science*, 2332:65–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320065.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320065.pdf.

Diffie:1998:PLP

[DL98] Whitfield Diffie and Susan Eva Landau. *Privacy on the Line: the Politics of Wiretapping and Encryption*. MIT Press, Cambridge, MA, USA, 1998. ISBN 0-262-04167-7 (hardcover). ix + 342 pp. LCCN KF9670 .D54 1998.

deLeeuw:2000:CSD

[dL00] Karl de Leeuw. *Cryptology and statecraft in the Dutch Republic [Cryptologie en buitenlands beleid in de Republiek der Verenigde Nederlanden]*. Ph.D. thesis, Universiteit van Amsterdam, Amsterdam, The Netherlands, 2000. viii + 190 pp. The work in this thesis has been carried out under the auspices of the research school IPA (Institute for Programming research and Algorithmics). In Dutch and English.

Diffie:2007:PLP

[DL07] Whitfield Diffie and Susan Eva Landau. *Privacy on the line: the politics of wiretapping and encryption*. MIT Press, Cambridge, MA, USA, updated and expanded edition, 2007. ISBN 0-262-04240-1. 400 (est.) pp. LCCN UB256.U6 D54 2007. URL http://www.loc.gov/catdir/toc/ecip073/2006035514.html.

deLeeuw:2007:HIS

[dLB07] Karl de Leeuw and J. A. Bergstra, editors. *The History of Information Security: a Comprehensive Handbook*. Elsevier, Amsterdam, The Netherlands, 2007. ISBN 0-444-51608-5 (hardcover). xi + 887 pp. LCCN Z103 .H63 2007.

DelLungo:2005:GSP

[DLMM05] Alberto Del Lungo, Guy Louchard, Claudio Marini, and Franco Montagna. The Guessing Secrets problem: a probabilistic approach. *Journal of Algorithms*, 55 (2):142–176, May 2005. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0196677404000422.

Daemen:2009:CAE

[DLP+09] Joan Daemen, Mario Lamberger, Norbert Pramstaller, Vincent Rijmen, and Frederik Vercauteren. Computational aspects of the expected differential probability of 4-round AES and AES-like ciphers. *Computing*, 85(1–2):85–104, June 2009. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=85&issue=1&spage=85.

Dodis:2008:OFE

[DLY08] Y. Dodis, P. J. Lee, and D. H. Yum. Optimistic fair exchange in a multi-user setting. *J.UCS: Journal of Universal Computer Science*, 14(3):318–346, ???? 2008. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_14_3/optimistic_fair_exchange_in.

DeSantis:2000:SSS

[DM00a] Alfredo De Santis and Barbara Masucci. On secret set schemes. *Information Processing Letters*, 74(5–6):243–251, June 30, 2000. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.nl/gej-ng/10/23/20/63/28/34/abstract.html; http://www.elsevier.nl/gej-ng/10/23/20/63/28/34/article.pdf.

Dodis:2000:PRI

[DM00b] Yevgeniy Dodis and Silvio Micali. Parallel reducibility for information-theoretically secure computation. In Bellare [Bel00], pages 74–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800074.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800074.pdf.

DeSantis:2007:NRN

[DM07a] Alfredo De Santis and Barbara Masucci. New results on non-perfect sharing of multiple secrets. *The Journal of Systems and Software*, 80(2):216–223, February 2007. CODEN JS-

SODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Drimer:2007:KYE

[DM07b] Saar Drimer and Steven J. Murdoch. Keep your enemies close: Distance bounding against Smartcard relay attacks. Report ??, Computer Laboratory, University of Cambridge, Cambridge, UK, May 15, 2007. 16 pp. URL http://www.cl.cam.ac.uk/~sd410/papers/sc_relay.bib. Also published in USENIX Security Symposium, August 2007, pages 87–102.

Dumais:2000:PCQ

[DMS00] Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. *Lecture Notes in Computer Science*, 1807: 300–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070300.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070300.pdf.

Dowd:2007:ASS

[DMS07] Mark Dowd, John McDonald, and Justin Schuh. *The art of software security assessment: identifying and preventing software vulnerabilities*. Addison-Wesley, Reading, MA, USA, 2007. ISBN 0-321-44442-6 (paperback). xxi + 1174 pp. LCCN QA76.9.A25 D75 2007. URL http://www.loc.gov/catdir/toc/ecip0618/2006023446.html.

Denev:2009:SFQ

[DMSW09] Dimitar Denev, Arturas Mazeika, Marc Spaniol, and Gerhard Weikum. SHARC: framework for quality-conscious Web archiving. *Proceedings of the VLDB Endowment*, 2(1):586–597, August 2009. CODEN ???? ISSN 2150-8097.

Ding:2007:ESD

[DMT07] Xuhua Ding, Daniele Mazzocchi, and Gene Tsudik. Equipping smart devices with public key signatures. *ACM Transactions on Internet Technology (TOIT)*, 7 (1):3:1–3:??, February 2007. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Damgaard:2000:INC

[DN00a] Ivan Damgård and Jesper Buus Nielsen. Improved non-committing encryption schemes based on a general complexity assumption. In Bellare [Bel00], pages 432–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800432.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800432.pdf.

Durfee:2000:CRS

[DN00b] Glenn Durfee and Phong Q. Nguyen. Cryptanalysis of the RSA schemes with short secret exponent from Asiacrypt '99. *Lecture Notes in Computer Science*, 1976: 14–29, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760014.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760014.pdf.

Damgaard:2002:EPF

[DN02a] Ivan Damgård and Jesper Buus Nielsen. Expanding pseudorandom functions; or: From known-plaintext security to chosen-plaintext security. In Yung [Yun02a], pages 449–464. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Damgaard:2002:PHP

[DN02b] Ivan Damgård and Jesper Buus Nielsen. Perfect hiding and perfect binding universally composable commitment schemes with constant expansion factor. In Yung [Yun02a], pages 581–596. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420565.htm; http://link.springer.de/link/service/series/0558/bibs/2442/24420581.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420565.pdf; http://link.springer.de/link/service/series/0558/papers/2442/24420581.pdf.

Damgaard:2003:UCE

[DN03] Ivan Damgård and Jesper Buus Nielsen. Universally composable efficient multiparty computation from threshold homomorphic encryption. In Boneh [Bon03], pages 247–

264. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Dwork:2004:PPD

[DN04] Cynthia Dwork and Kobbi Nissim. Privacy-preserving datamining on vertically partitioned databases. In Franklin [Fra04], pages 528–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Doncel:2007:ODS

[DNP07] Victor Rodriguez Doncel, Nikos Nikolaidis, and Ioannis Pitas. An optimal detector structure for the Fourier descriptors domain watermarking of 2D vector graphics. *IEEE Transactions on Visualization and Computer Graphics*, 13(5):851–863, September/October 2007. CODEN ITVGEA. ISSN 1077-2626 (print), 1941-0506 (electronic), 2160-9306.

Dwork:2003:MFM

[DNRS03] Cynthia Dwork, Moni Naor, Omer Reingold, and Larry Stockmeyer. Magic functions: In memoriam: Bernard M. Dwork 1923–1998. *Journal of the ACM*, 50(6):852–921, November 2003. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Dwork:2005:PPW

[DNW05] Cynthia Dwork, Moni Naor, and Hoeteck Wee. Pebbling and proofs of work. In Shoup [Sho05a], pages 37–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Dodis:2005:GIF

[DOP05] Yevgeniy Dodis, Roberto Oliveira, and Krzysztof Pietrzak. On the generic insecurity of the full domain hash. In Shoup [Sho05a], pages 449–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Dodis:2004:IPC

[DOPS04] Y. Dodis, Shien Jin Ong, M. Prabhakaran, and A. Sahai. On the (im)possibility of cryptography with imperfect randomness. In IEEE [IEE04], pages 196–205. CODEN ASFPDV. ISBN 0-7695-2228-9. ISSN 0272-5428. LCCN QA276. URL http://ieeexplore.ieee.org/iel5/9430/29918/01366239.pdf?isnumber=29918&prod=CNF&arnumber=1366239&arSt=+196&ared=+205&arAuthor=Dodis%2C+Y.%3B+Shien+Jin+Ong%3B+Prabhakaran%2C+M.%3B+Sahai%2C+A.; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=29918&arnumber=1366239&count=64&index=20. IEEE Computer Society Order Number P2228.

Dhamija:2000:DVU

[DP00] Rachna Dhamija and Adrian Perrig. Déjà Vu — A user study: Using images for authentication. In USENIX [USE00d], page ?? ISBN 1-880446-18-9. LCCN ???? URL http://www.usenix.org/publications/library/proceedings/sec2000/dhamija.html.

DeMatteis:2002:PP

[DP02] A. De Matteis and S. Pagnutti. Pseudorandom permutation. *Journal of Computational and Applied Mathematics*, 142(2):367–375, May 15, 2002. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042701004253.

Dandalis:2004:ACE

[DP04] Andreas Dandalis and Viktor K. Prasanna. An adaptive cryptographic engine for Internet protocol security architectures. *ACM Transactions on Design Automation of Electronic Systems*, 9(3):333–353, July 2004. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Dziembowski:2007:IRS

[DP07] S. Dziembowski and K. Pietrzak. Intrusion-resilient secret sharing. In IEEE [IEE07], pages 227–237. ISBN 0-7695-3010-9. ISSN 0272-5428. LCCN QA76 .S974 2007. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4389466.

IEEE Computer Society order number P3010.

Dziembowski:2008:LRC

[DP08] S. Dziembowski and K. Pietrzak. Leakage-resilient cryptography. In IEEE [IEE08], pages 293–302. ISBN 0-7695-3436-8. ISSN 0272-5428. LCCN QA76 .S95 2008. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4690923. IEEE Computer Society order number P3436.

Dandalis:2001:CSP

[DPR01] Andreas Dandalis, Viktor K. Prasanna, and Jose D. P. Rolim. A comparative study of performance of AES final candidates using FPGAs. *Lecture Notes in Computer Science*, 1965:125–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650125.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650125.pdf.

Damgaard:2005:QCN

[DPS05] Ivan Damgård, Thomas Brochmann Pedersen, and Louis Salvail. A quantum cipher with near optimal key-recycling. In Shoup [Sho05a], pages 494–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Delbourg:2002:JBC

[DPT+02] D. Delbourg, G. Penillault, T. K. Tuong, M. Decourt, N. Borome, H. Harroch, B. Lessellier, B. Waast, and J. P. Mouffron. A Java-based control system for the Orsay tandem accelerator. *Pramana: Journal of Physics*, 59(6):1025–1034, 2002. CODEN PRAMCI. ISSN 0304-4289.

Daemen:2001:BCP

[DPV01] Joan Daemen, Michael Peeters, and Gilles Van Assche. Bitslice ciphers and power analysis attacks. *Lecture Notes in Computer Science*, 1978:134–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780134.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780134.pdf.

Crescenzo:2004:CRR

[DPV04] Giovanni Di Crescenzo, Giuseppe Persiano, and Ivan Visconti. Constant-round resettable zero knowledge with concurrent soundness in the bare public-key model. In Franklin [Fra04], pages 237–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Daemen:2000:NPN

[DPVR00] Joan Daemen, Michaël Peeters, Gilles Van Assche, and Vincent Rijmen. Nessie proposal: NOEKEON. Report, Proton World International and ESAT Cosic KULeuven, Belgium, October 27, 2000. 30 pp. URL http://gro.noekeon.org/Noekeon-spec.pdf.

Daemen:2000:BCR

[DR00a] Joan Daemen and Vincent Rijmen. The block cipher Rijndael. In Quisquater and Schneier [QS00], pages 288–296. ISBN 3-540-67923-5. LCCN TK7895.S62 C36 1998.

Daemen:2000:RA

[DR00b] Joan Daemen and Vincent Rijmen. Rijndael for AES. In NIST [NIS00], pages 343–347. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

DDJ:2000:DDE

[Dr.00c] Dr.Dobb's Journal. Dr. Dobb's essential books on cryptography and security. CD-ROM containing PDF files., 2000. URL http://www.ddj.com/cdrom/; http://www.digitalriver.com/dr/v2/ec_MAIN.Entry10?SP=10023&PN=1&V1=163454&xid=2823. Includes twelve books on cryptography.

Daemen:2001:AAR

[DR01] Joan Daemen and Vincent Rijmen. Algorithm alley: Rijndael: The Advanced Encryption Standard. *Dr. Dobb's Journal of Software Tools*, 26(3):

137–139, March 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ftp/2001/2001_03/aa0301.txt; http://www.esat.kuleuven.ac.be/~rijmen/rijndael/.

Daemen:2002:AWT

[DR02a] Joan Daemen and Vincent Rijmen. AES and the wide trail design strategy. *Lecture Notes in Computer Science*, 2332:108–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320108.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320108.pdf.

Daemen:2002:DRA

[DR02b] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES – The Advanced Encryption Standard*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. ISBN 3-642-07646-7, 3-662-04722-5 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xvii + 238 pp. LCCN QA76.9.A25. URL http://www.springerlink.com/content/978-3-662-04722-4.

Daemen:2002:FSE

[DR02c] Joan Daemen and Vincent Rijmen, editors. *Fast Software Encryption: 9th International Workshop, FSE 2002, Leuven, Belgium, February 4–6, 2002. Revised Papers*, volume 2365 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-44009-7 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F77 2002b. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2365.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2365.

Ding:2002:HEE

[DR02d] Yan Zong Ding and Michael O. Rabin. Hyper-encryption and everlasting security. *Lecture Notes in Computer Science*, 2285:1–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2285/22850001.htm; http://link.springer-ny.com/link/service/series/

0558/papers/2285/22850001.pdf.

Dray:2000:NPA

[Dra00] Jim Dray. NIST performance analysis of the final round Java AES candidates. In NIST [NIS00], pages 149–160. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Dreyfus:2000:PUC

[Dre00] Suelette Dreyfus. The practical use of cryptography in human rights groups, 2000. URL http://www.usenix.org/publications/library/proceedings/sec2000/invitedtalks.html. Unpublished invited talk at Ninth USENIX Security Symposium.

Driscoll:2002:BER

[Dri02] Kevin Driscoll. BeepBeep: Embedded real-time encryption. *Lecture Notes in Computer Science*, 2365: 164–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650164.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650164.pdf.

Diqun:2009:QSP

[DRL09] Yan Diqun, Wang Rangding, and Zhang Liguang. Quantization step parity-based steganography for MP3 audio. *Fundamenta Informaticae*, 97(1–2):1–14, January 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

delRey:2005:SSS

[dRMS05] A. Martín del Rey, J. Pereira Mateus, and G. Rodríguez Sánchez. A secret sharing scheme based on cellular automata. *Applied Mathematics and Computation*, 170(2):1356–1364, November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300305000718.

Dobbertin:2005:AES

[DRS05] Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa, editors. *Advanced en-*

cryption standard — AES: 4th international conference, AES 2004, Bonn, Germany, May 10–12, 2004, revised selected and invited papers, volume 3373 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-26557-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3373`.

Devanbu:2000:CVT

[DS00] P. T. Devanbu and S. G. Stubblebine. Cryptographic verification of test coverage claims. *IEEE Transactions on Software Engineering*, 26(2):178–192, February 2000. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=841116`.

Dodis:2002:NUO

[DS02] Y. Dodis and J. Spencer. On the (non)universality of the one-time pad. In IEEE [IEE02], pages 376–385. CODEN ASFPDV. ISBN 0-7695-1822-2. ISSN 0272-5428. LCCN QA267. URL `http://ieeexplore.ieee.org/iel5/8411/26517/01181962.pdf?isnumber=26517&prod=CNF&arnumber=1181962&arSt=+376&ared=+385&arAuthor=Dodis%2C+Y.%3B+Spencer%2C+J.`; `http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=26517&arnumber=1181962&count=82&index=38`. IEEE Computer Society Order Number PR01822.

DArco:2003:FTD

[DS03] Paolo D'Arco and Douglas R. Stinson. Fault tolerant and distributed broadcast encryption. In Joye [Joy03b], pages 263–280. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612`.

Ding:2005:RNM

[DS05a] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. *Lecture Notes in Computer Science*, 3531: 164–175, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dodis:2005:ESE

[DS05b] Yevgeniy Dodis and Adam Smith. Entropic security and the encryption of high entropy messages. In Kilian [Kil05], pages 556–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Ding:2006:SSS

[DS06] Cunsheng Ding and Arto Salomaa. Secret sharing schemes with nice access structures. *Fundamenta Informaticae*, 73(1–2):51–63, October 2006. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Dinur:2008:CAT

[DS08] Itai Dinur and Adi Shamir. Cube attacks on tweakable black box polynomials. Technical report, Computer Science Department, The Weizmann Institute, Rehobot 76100, Israel, September 13, 2008. URL http://cryptome.org/cube-attacks.pdf.

Deepthi:2009:DIA

[DS09] P. P. Deepthi and P. S. Sathidevi. Design, implementation and analysis of hardware efficient stream ciphers using LFSR based hash functions. *Computers & Security*, 28(3–4):229–241, May/June 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808001193.

Das:2006:NRU

[DSGP06] Manik Lal Das, Ashutosh Saxena, Ved P. Gulati, and Deepak B. Phatak. A novel remote user authentication scheme using bilinear pairings. *Computers & Security*, 25(3):184–189, May 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404805001525.

Djurovic:2001:DWF

[DSP01] Igor Djurovic, Srdjan Stankovic, and Ioannis Pitas. Digital watermarking in the fractional Fourier transformation domain. *Journal of Network and Computer Applications*, 24(2):167–173, April 2001. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S1084804500901280.

Dodis:2001:PAS

[DSS01] Yevgeniy Dodis, Amit Sahai, and Adam Smith. On perfect and adaptive security in exposure-resilient cryptography. *Lecture Notes in Computer Science*, 2045: 301–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450301.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450301.pdf.

Ding:2003:SIB

[DT03] Xuhua Ding and Gene Tsudik. Simple identity-based cryptography with mediated RSA. In Joye [Joy03b], pages 193–210. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Duggan:2004:TBC

[Dug04] Dominic Duggan. Type-based cryptographic operations. *Journal of Computer Security*, 12(3–4):485–550, ???? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dujella:2008:VWA

[Duj08] Andrej Dujella. A variant of Wiener's attack on RSA with small secret exponent. *ACM Communications in Computer Algebra*, 42(1–2):50–51, March/June 2008. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Dujella:2009:VWA

[Duj09] Andrej Dujella. A variant of Wiener's attack on RSA. *Computing*, 85(1–2):77–83, June 2009. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=85&issue=1&spage=77.

Dunkelman:2006:TCB

[Dun06] Orr Dunkelman. *Techniques for cryptanalysis of block ciphers*. Thesis (Ph.D.), Faculty of Computer Science, Technion — Israel Institute of Technology, Haifa, Israel, 2006. x + 204 pp.

Duranti:2001:LTP

[Dur01] Luciana Duranti. The long-term preservation of authentic electronic records. In Apers et al. [AAC+01], pages 625–628. ISBN 1-55860-804-4. LCCN QA76.9.D3 I559 2001. URL http://www.vldb.org/conf/2001/P625.pdf.

Duwell:2003:BRB

[Duw03] Armond Duwell. Book review: *The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation*: D. Bouwmeester, A. Ekert and A. Zeilinger (Eds.); Germany, 2000, 314pp, US$54, ISBN 3-540-66778-4. *Studies in History and Philosophy of Modern Physics*, 34(2):331–334, June 2003. CODEN ???? ISSN 1355-2198 (print), 1879-2502 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1355219803000121. See [BEZ01].

Dawson:2005:PCM

[DV05] Ed Dawson and Serge Vaudenay, editors. *Progress in cryptology — MYCRYPT 2005: first international conference on cryptology in Malaysia, Kuala Lumpur, Malaysia, September 28–30, 2005, proceedings*, volume 3715 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-28938-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ????

Drutarovsky:2008:CSC

[DV08] M. Drutarovsky and M. Varchola. Cryptographic system on a chip based on Actel ARM7 soft-core with embedded true random number generator. In *2008. DDECS 2008. 11th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4538778.

Levy-dit-Vehel:2006:WC

[dVP06] Françoise Levy dit Vehel and Ludovic Perret. On the Wagner–Magyarik cryptosystem. In Ytrehus [Ytr06], pages 316–329. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Doyle:2009:LTD

[DVP09] Julie Doyle, Herna Viktor, and Eric Paquet. Long-term digital preservation: preserving authenticity and usability of 3-D data. *International Journal on Digital Libraries*, 10(1):33–47, May 2009. CODEN ???? ISSN

1432-1300 (print), 1432-5012 (electronic). URL https://link.springer.com/article/10.1007/s00799-009-0051-7.

Du:2001:OKS

[DW01] Wei Zhang Du and Xin Mei Wang. One kind of secret-code encryption scheme based on maximum rank distance codes. *Chinese Journal of Computers = Chi suan chi hsueh pao*, 24(6): 650–653, 2001. CODEN JIXUDT. ISSN 0254-4164.

deWeger:2002:CRS

[dW02] Benne de Weger. Cryptanalysis of RSA with small prime difference. *Applicable algebra in engineering, communication and computing*, 13(1):17–28, 2002. CODEN AAECEW. ISSN 0938-1279 (print), 1432-0622 (electronic).

Ding:2005:CTC

[DW05] Cunsheng Ding and Xuesong Wang. A coding theory construction of new systematic authentication codes. *Theoretical Computer Science*, 330(1):81–99, January 31, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Dodis:2009:NME

[DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In ACM [ACM09], pages 601–610. ISBN 1-60558-613-7. LCCN QA75.5 .A22 2009.

Dwivedi:2004:ISS

[Dwi04] Himanshu Dwivedi. *Implementing SSH: strategies for optimizing the secure shell*. John Wiley and Sons, Inc., New York, NY, USA, 2004. ISBN 0-471-45880-5. xxvi + 376 pp. LCCN QA76.76.O63 D895 2004. UK£24.50. URL ftp://uiarchive.cso.uiuc.edu/pub/etext/gutenberg/; http://www.loc.gov/catdir/bios/wiley046/2004297174.html; http://www.loc.gov/catdir/description/wiley041/2004297174.html; http://www.loc.gov/catdir/toc/wiley041/2004297174.html.

Desmedt:2005:CNS

[DWML05] Yvo G. Desmedt, Huaxiong Wang, Yi Mu, and Yongqing Li, editors. *Cryptology and network security: 4th international conference, CANS 2005, Xiamen, China, December 14–16, 2005: proceedings*, volume 3810 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-30849-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I5534 2004. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3810.

Dittmann:2001:UCW

[DWN01] Jana Dittmann, Petra Wohlmacher, and Klara Nahrstedt. Using cryptographic and watermarking algorithms. *IEEE MultiMedia*, 8(4):54–65, October 2001. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://dlib.computer.org/mu/books/mu2001/pdf/u4054.pdf; http://www.computer.org/multimedia/mu2001/u4054abs.htm.

Dworkin:2003:DRB

[Dwo03] Morris Dworkin. DRAFT recommendation for block cipher modes of operation: The CCM mode for authentication and confidentiality. NIST Special Publication 800-38C, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, September 2003. URL http://csrc.nist.gov/publications/drafts/Draft_SP_800-38C_9-04-2003.pdf.

Ding:2005:NME

[DwWmW05] Yong Ding, Kwok wo Wong, and Yu min Wang. A w-NNAF method for the efficient computation of scalar multiplication in elliptic curve cryptography. *Applied Mathematics and Computation*, 167(1):81–93, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Dawu:2001:TES

[DY01] Gu Dawu and Wang Yi. On the techniques of enhancing the security of block ciphers. *Operating Systems Review*, 35(4):94–96, October 2001. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Deng:2009:SCA

[DY09a] Robert H. Deng and Yanjiang Yang. A study of content authentication in proxy-enabled multimedia delivery systems: Model, techniques, and applications. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 5(4):28:1–28:??, October 2009. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Ding:2009:MPK

[DY09b] Jintai Ding and Bo-Yin Yang. Multivariate public key cryptography. In Bernstein et al. [BBD09], pages 198–242. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Dai:2001:CDE

[DZL01] Qiong Dai, Xiao Xiang Zou, and Zhu Kai Luo. Cracking a data encryption and decryption system using multi-valued logic array. *Chinese Journal of Computers = Chi suan chi hsueh pao*, 24(6):654–656, 2001. CODEN JIXUDT. ISSN 0254-4164.

Eagleton:2005:BRD

[Eag05] Catherine Eagleton. Book review: David A. King, The Ciphers of the Monks: A Forgotten Number-Notation of the Middle Ages. Boethius, 44. Stuttgart: FranzSteiner Verlag, 2001. Pp. 506. ISBN 3-515-07640-9. DM 199.49, EUR 102.00 (hardcover). *British Journal for the History of Science*, 38(3):359–360, September 2005. CODEN BJHSAT. ISSN 0007-0874 (print), 1474-001X (electronic). URL http://www.jstor.org/stable/4028680.

ElAbbadi:2000:VPI

[EBC+00] Amr El Abbadi, Michael L. Brodie, Sharma Chakravarthy, Umeshwar Dayal, Nabil Kamel, Gunter Schlageter, and Kyu-Young Whang, editors. *VLDB 2000, Proceedings of 26th International Conference on Very Large Data Bases, September 10–14, 2000, Cairo, Egypt*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 2000. ISBN 1-55860-715-3. LCCN ????

Eghlidos:2001:IRL

[EBS01] Taraneh Eghlidos, Albrecht Beutelspacher, and Babak Sadeghiyan. Improving the resistance of DES and DES-like cryptosystems against differential cryptanalysis. *Atti Sem. Mat. Fis. Univ. Modena*, 49(1):147–169, 2001. CODEN ASMMAK. ISSN 0041-8986.

Eilam:2005:RSR

[EC05] Eldad Eilam and Elliot J. Chikofsky. *Reversing: secrets of reverse engineering*. John Wiley and Sons, Inc., New York, NY, USA, 2005. ISBN 0-7645-7481-7 (paperback). xxviii + 589 pp. LCCN QA76.758 .E35 2005. URL http://www.loc.gov/catdir/enhancements/fy0628/2005921595-b.html; http://www.loc.gov/catdir/enhancements/fy0628/2005921595-d.html; http://www.loc.gov/catdir/enhancements/fy0628/2005921595-t.html.

English:2007:MAC

[ECG+07] Jennifer English, David Coe, Rhonda Gaede, David Hyde, and Jeffrey Kulick. MEMS-assisted cryptography for CPI protection.

IEEE Security & Privacy, 5(4):14–21, July/August 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

ECMA:2000:EPIa

[ECM00a] ECMA. *ECMA-305: Private Integrated Services Network (PISN) — Specification, Functional Model and Information Flows — Wireless Terminal Authentication Supplementary Services (WTMAU-SD)*. ECMA (European Association for Standardizing Information and Communication Systems), Geneva, Switzerland, June 2000. URL http://www.ecma.ch/ecma1/STAND/ECMA-305.HTM.

ECMA:2000:EPIb

[ECM00b] ECMA. *ECMA-306: Private Integrated Services Network (PISN) — Inter-Exchange Signalling Protocol — Wireless Terminal Authentication Supplementary Services (QSIG-WTMAU)*. ECMA (European Association for Standardizing Information and Communication Systems), Geneva, Switzerland, June 2000. URL http://www.ecma.ch/ecma1/STAND/ECMA-306.HTM.

Ellison:2003:PKS

[ED03] Carl Ellison and Steve Dohrmann. Public-key support for group collaboration. *ACM Transactions on Information and System Security*, 6(4):547–565, November 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Echizen:2005:PAV

[EFY+05] Isao Echizen, Yasuhiro Fujii, Takaaki Yamada, Satoru Tezuka, and Hiroshi Yoshiura. Perceptually adaptive video watermarking using motion estimation. *International Journal of Image and Graphics (IJIG)*, 5(1):89–??, January 2005. CODEN ???? ISSN 0219-4678.

Eghlidos:2000:SLB

[Egh00] Taraneh Eghlidos. *On the security of DES and DES-like block ciphers against differential cryptanalysis*. Shaker Verlag, Aachen, Germany, 2000. ISBN 3-8265-7951-8. xvi + 178 pp. LCCN ????

Elmallah:2008:LK

[EGK08] Ehab S. Elmallah, Mohamed G. Gouda, and Sandeep S. Kulkarni. Logarithmic keying. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 3(4):18:1–18:??, November 2008. CODEN ???? ISSN 1556-4665 (print), 1556-4703 (electronic).

Epstein:2003:DIT

[EHK+03] Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner, and Hao Zheng. Design and implementation of a true random number generator based on digital circuit artifacts. In Walter et al. [WKP03], pages 152–165. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Ernst:2004:FBH

[EHKH04] M. Ernst, B. Henhapl, S. Klupsch, and S. Huss. FPGA based hardware acceleration for elliptic curve public key cryptosystems. *The Journal of Systems and Software*, 70(3):299–313, March 2004. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Ellison:2000:PSK

[EHMS00] Carl Ellison, Chris Hall, Randy Milbert, and Bruce Schneier. Protecting secret keys with personal entropy. *Future Generation Computer Systems*, 16(4):311–318, February 2000. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.counterpane.com/personal-entropy.pdf; http://www.elsevier.com/gej-ng/10/19/19/41/27/26/abstract.html.

Eggers:2001:DWC

[EIG01] Joachim J. Eggers, Wolf-Dietrich Ihlenfeldt, and Bernd Girod. Digital watermarking of chemical structure sets. *Lecture Notes in Computer Science*, 2137: 200–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370200.htm; http://link.springer-ny.com/link/service/series/0558/papers/2137/21370200.pdf.

Ekert:2002:BTQ

[Eke02] Artur Ekert. 29. The Bell Theorem in quantum cryptography: Vortrag am 14. November 2000. In Bertlmann and Zeilinger [BZ02], page ?? ISBN 3-540-42756-2. LCCN ????

Ekeraa:2009:DCM

[Eke09] Martin Ekerå. *Differential cryptanalysis of MD5.*

Ph.D. thesis (??), Skolan för datavetenskap och kommunikation, Kungliga Tekniska högskolan, Stockholm, Sweden, 2009. 113 pp.

El-Kassar:2001:GPK

[EKRMA01] A. N. El-Kassar, Mohamed Rizk, N. M. Mirza, and Y. A. Awad. El-Gamal public key cryptosystem in the domain of Gaussian integers. *Int. J. Appl. Math.*, 7(4):405–412, 2001. ISSN 1311-1728.

Elbirt:2008:AAI

[Elb08] A. J. Elbirt. Accelerated AES implementations via generalized instruction set extensions. *Journal of Computer Security*, 16 (3):265–288, ???? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Elbirt:2009:UAC

[Elb09] Adam J. Elbirt. *Understanding and Applying Cryptography and Data Security*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 2009. ISBN 1-4200-6160-7. xxvii + 637 pp. LCCN QA76.9.A25 E43 2009. URL http://www.loc.gov/catdir/toc/ecip0821/2008028154.html.

Elliott:2004:QC

[Ell04] Chip Elliott. Quantum cryptography. *IEEE Security & Privacy*, 2(4):57–61, July/August 2004. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://csdl.computer.org/dl/mags/sp/2004/04/j4057.htm; http://csdl.computer.org/dl/mags/sp/2004/04/j4057.pdf.

Eloff:2001:AIS

[ELvS01] Jan H. P. Eloff, Les Labuschagne, and Rossouw von Solms, editors. *Advances in Information Security Management and Small Systems Security: IFIP TC11 WG11.1/WG11.2 Eighth Annual Working Conference on Information Security Management and Small Systems Security, September 27–28, 2001, Las Vegas, Nevada, USA*, volume 72 of *International Federation for Information Processing*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2001. ISBN 0-7923-7506-8. LCCN QA76.9.A25 I465 2001. UK£97.00.

Everitt:2003:JBI

[EM03] R. A. J. Everitt and P. W. McOwan. Java-based Internet biometric authentication system. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(9):1166–1171, 2003. CODEN ???? ISSN 0162-8828.

English:2000:MNDb

[Eng00] Marie English. Micro news: Digital-signature legislation. *IEEE Micro*, 20(4):4, July/ August 2000. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

England:2002:AOO

[EP02] Paul England and Marcus Peinado. Authenticated operation of open computing devices. *Lecture Notes in Computer Science*, 2384:346–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840346.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2384/23840346.pdf`.

Elbirt:2005:ILD

[EP05] Adam J. Elbirt and Christof Paar. An instruction-level distributed processor for symmetric-key cryptography. *IEEE Transactions on Parallel and Distributed Systems*, 16(5):468–480, May 2005. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Eisenbarth:2007:SLC

[EPP+07] Thomas Eisenbarth, Christof Paar, Axel Poschmann, Sandeep Kumar, and Leif Uhsadel. A survey of lightweight cryptography implementations. *IEEE Design & Test of Computers*, 24(6):522–533, November/December 2007. ISSN 0740-7475 (print), 1558-1918 (electronic).

Erickson:2001:EDD

[Eri01] Jonathan Erickson. Editorial: From the Department of Dumb Ideas. *Dr. Dobb's Journal of Software Tools*, 26(3):8, March 2001. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/`.

Erickson:2002:EDD

[Eri02] Jonathan Erickson. Editorial: Deciphering the doors of knowledge. *Dr. Dobb's Journal of Software Tools*, 27(4):8, April 2002. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/`.

Erickson:2003:HAE

[Eri03] Jon (Jon Mark) Erickson. *Hacking: the art of exploitation.* No Starch Press, San Francisco, CA, USA, 2003. ISBN 1-59327-007-0. xi + 241 pp. LCCN QA76.9.A25 E75 2003. URL `http://www.loc.gov/catdir/toc/ecip047/2003017498.html`.

Erickson:2008:HAE

[Eri08] Jon Erickson. *Hacking: the art of exploitation*. No Starch Press, San Francisco, CA, USA, second edition, 2008. ISBN 1-59327-144-1. x + 472 pp. LCCN QA76.9.A25 E75 2008. URL http://proquest.safaribooksonline.com/9781593271442.

Ellison:2000:TRP

[ES00a] C. Ellison and B. Schneier. Ten risks of PKI: What you're not being told about public-key infrastructure. *Computer Security Journal*, 16(1):1–7, ???? 2000. CODEN CSJLDR. ISSN 0277-0865.

Ellison:2000:IRRa

[ES00b] Carl Ellison and Bruce Schneier. Inside risks: risks of PKI: Secure email. *Communications of the Association for Computing Machinery*, 43(1):160, January 2000. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/articles/journals/cacm/2000-43-1/p160-ellison/p160-ellison.pdf; http://www.acm.org/pubs/citations/journals/cacm/2000-43-1/p160-ellison/.

Eberle:2005:ANG

[ESG+05] Hans Eberle, Sheueling Shantz, Vipul Gupta, Nils Gura, Leonard Rarick, and Lawrence Spracklen. Accelerating next-generation public-key cryptosystems on general-purpose CPUs. *IEEE Micro*, 25(2):52–59, March/April 2005. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://csdl.computer.org/comp/mags/mi/2005/02/m2052abs.htm; http://csdl.computer.org/dl/mags/mi/2005/02/m2052.pdf.

Enck:2005:EOF

[ETMP05] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting open functionality in SMS-capable cellular networks. In Meadows and Syverson [MS05b], pages 393–404. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Ettinger:2002:QQC

[Ett02] Mark Ettinger. 20 questions, quantum computers, and cryptography. *Los Alamos Science*, 27:46–51, 2002. CODEN LASCDI. ISSN 0273-7116.

Ebringer:2000:PAP

[ETZ00] Tim Ebringer, Peter Thorne, and Yuliang Zheng. Parasitic authentication to protect your E-wallet. *Computer*, 33(10):54–60, October 2000. CODEN CP-

TRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co2000/pdf/rx054.pdf; http://www.computer.org/computer/co2000/rx054abs.htm.

Evans:2009:BRS

[Eva09] James Evans. Book review: The saga of the Antikythera mechanism, *Decoding the Heavens: a 2000-Year-Old Computer and the Century-Long Search to Discover its Secrets*. *Journal for the History of Astronomy*, 40 (3):362–364, August 2009. CODEN JHSAA2. ISSN 0021-8286 (print), 1753-8556 (electronic).

Edman:2009:AES

[EY09] Matthew Edman and Bülent Yener. On anonymity in an electronic society: a survey of anonymous communication systems. *ACM Computing Surveys*, 42(1):5:1–5:35, December 2009. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Elbirt:2000:FIP

[EYCP00] A. J. Elbirt, W. Yip, B. Chetwynd, and C. Paar. An FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalists. In NIST [NIS00], pages 13–27. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Faliszewski:2007:BRB

[Fal07] Piotr Faliszewski. Book review: *Complexity Theory and Cryptology: An Introduction to Cryptocomplexity*, by Jörg Rothe, Springer, 2005, 484 pages. *ACM SIGACT News*, 38(2):20–22, June 2007. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL http://doi.acm.org/10.1145/1272729.1272736. See [Rot05].

Fan:2003:ILC

[Fan03] Chun-I Fan. Improved low-computation partially blind signatures. *Applied Mathematics and Computation*, 145(2–3):853–867, December 25, 2003. CODEN AMHCBQ. ISSN 0096-3003

(print), 1873-5649 (electronic).

Faugere:2009:IBC

[Fau09] Jean-Charles Faugère. Interactions between computer algebra (Gröbner bases) and cryptology. In May [May09], pages 383–384. ISBN 1-60558-609-9. LCCN ????

Ford:2001:SEC

[FB01] Warwick Ford and Michael S. Baum. *Secure electronic commerce: building the infrastructure for digital signatures and encryption*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, second edition, 2001. ISBN 0-13-203795-5 (paperback). xxv + 612 pp. LCCN QA76.9.A25 F655 2000.

Felkel:2001:ICW

[FBW01] Petr Felkel, Mario Bruckschwaiger, and Rainer Wegenkittl. Implementation and complexity of the watershed-from-markers algorithm computed as a minimal cost forest. *Computer Graphics Forum*, 20(3):??, September 2001. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Feghali:2002:SAP

[FBWC02] Wajdi Feghali, Brad Burres, Gilbert Wolrich, and Douglas Carrigan. Security: Adding protection to the network via the network processor. *Intel Technology Journal*, 6(3):40–49, August 15, 2002. ISSN 1535-766X. URL http://developer.intel.com/technology/itj/2002/volume06issue03/art02_security/p01_abstract.htm; http://developer.intel.com/technology/itj/2002/volume06issue03/art02_security/vol6iss3_art02.pdf.

Fan:2005:RRA

[FCZ05] Chun-I Fan, Yung-Cheng Chan, and Zhi-Kai Zhang. Robust remote authentication scheme with smart cards. *Computers & Security*, 24(8):619–628, November 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404805000477.

Fischer:2001:TMR

[FD01] V. Fischer and M. Drutarovský. Two methods of Rijndael implementation in reconfigurable hardware. *Lecture Notes in Computer Science*, 2162: 77–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620077.htm; http://link.springer-

ny.com/link/service/series/0558/papers/2162/21620077.pdf.

Furnell:2000:ASS

[FDIR00] S. M. Furnell, P. S. Dowland, H. M. Illingworth, and P. L. Reynolds. Authentication and supervision: a survey of user attitudes. *Computers & Security*, 19(6):529–539, October 1, 2000. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404800060272.

Felke:2006:ATH

[Fel06] Patrick Felke. On the affine transformations of HFE-cryptosystems and systems with branches. In Ytrehus [Ytr06], pages 229–241. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Ferguson:2000:SEK

[Fer00] N. Ferguson. Semi-equivalent keys in MARS. In ????, editor, *Third AES Candidate Conference*, page ?? ????, ????, April 2000. ISBN ???? LCCN ????

Ferguson:2006:ACE

[Fer06] Niels Ferguson. AES-CBC + Elephant diffuser: A disk encryption algorithm for Windows Vista. Unknown, 2006.

Fischlin:2000:ENM

[FF00] Marc Fischlin and Roger Fischlin. Efficient non-malleable commitment schemes. In Bellare [Bel00], pages 413–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800413.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800413.pdf.

Filiol:2001:NUS

[FF01a] Eric Filiol and Caroline Fontaine. A new ultrafast stream cipher design: COS ciphers. *Lecture Notes in Computer Science*, 2260:85–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600085.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600085.pdf.

Flannery:2001:CYW

[FF01b] Sarah Flannery and David Flannery. *In Code: a [Young Women's] Mathematical Journey*. Algonquin Books of Chapel Hill, Chapel Hill, NC, USA, 2001.

ISBN 1-56512-377-8. ix + 341 pp. LCCN QA29.F6 A3 2003. US$13.95.

Fridrich:2001:DLS

[FGD01] Jessica Fridrich, Miroslav Goljan, and Rui Du. Detecting LSB steganography in color and gray-scale images. *IEEE MultiMedia*, 8(4):22–28, October 2001. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL `http://dlib.computer.org/mu/books/mu2001/pdf/u4022.pdf`; `http://www.computer.org/multimedia/mu2001/u4022abs.htm`.

Frenkiel:2002:CCS

[FGL02] Michel Frenkiel, Paul Grison, and Philippe Laluyaux. Clip Card: Smart Card based traffic tickets. *Lecture Notes in Computer Science*, 2456:313–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2456/24560313.htm`; `http://link.springer.de/link/service/series/0558/papers/2456/24560313.pdf`.

Focardi:2000:ITN

[FGM00a] Riccardo Focardi, Roberto Gorrieri, and Fabio Martinelli. Invited talk: Non interference for the analysis of cryptographic protocols. *Lecture Notes in Computer Science*, 1853: 354–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1853/18530354.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1853/18530354.pdf`.

Focardi:2000:MAT

[FGM00b] Riccardo Focardi, Roberto Gorrieri, and Fabio Martinelli. Message authentication through non interference. *Lecture Notes in Computer Science*, 1816: 258–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1816/18160258.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1816/18160258.pdf`.

Focardi:2003:CTA

[FGM03] Riccardo Focardi, Roberto Gorrieri, and Fabio Martinelli. A comparison of three authentication properties. *Theoretical Computer Science*, 291(3):285–327, January 6, 2003. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Fitzi:2001:MCP

[FGMO01] Matthias Fitzi, Juan A. Garay, Ueli Maurer, and Rafail Ostrovsky. Minimal complete primitives for secure multi-party computation. In Kilian [Kil01a], pages 80–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390080.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390080.pdf`.

Field:2009:BCB

[Fie09] J. V. Field. British cryptanalysis : the breaking of 'fish' traffic. In *Scientific research in World War II: what scientists did in the war* [MH09], page ?? ISBN 0-203-88318-7 (e-book), 0-7103-1340-3 (hardcover). LCCN Q141 .H195 2009. URL `http://www.loc.gov/catdir/toc/ecip0824/2008033118.html`.

Filiol:2000:DAS

[Fil00] Eric Filiol. Decimation attack of stream ciphers. *Lecture Notes in Computer Science*, 1977:31–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1977/19770031.htm; http://link.springer-ny.com/link/service/series/0558/papers/1977/19770031.pdf`.

Filiol:2002:NST

[Fil02] Eric Filiol. A new statistical testing for symmetric ciphers and hash functions. Technical report, ESAT — Virology and Cryptology Lab, B.P. 18 35998 Rennes, FRANCE, July 23, 2002. 14 pp. URL `http://eprint.iacr.org/2002/099/`. Cryptology ePrint Archive, Report 2002/099.

Finley:2002:BSE

[Fin02] Brian Elliott Finley. BOEL: a small Embedded Linux with PIC libraries. *Embedded Linux Journal*, 8: 44–46, March/April 2002. CODEN ???? ISSN 1534-083X. URL `http://embedded.linuxjournal.com/magazine/issue08/; http://www.linuxdevices.com/articles/AT2829528599.html`.

Finkenzeller:2003:RHF

[Fin03] Klaus Finkenzeller. *RFID handbook: fundamentals and applications in contactless smart cards and identification*. John Wiley and Sons, Inc., New York, NY, USA, second edition, 2003. ISBN 0-470-84402-7. xviii

+ 427 pp. LCCN TS160 .F5513 2003. URL ftp://uiarchive.cso.uiuc.edu/pub/etext/gutenberg/; http://www.loc.gov/catdir/description/wiley039/2002192439.html; http://www.loc.gov/catdir/toc/wiley031/2002192439.html.

Finnigin:2006:CPN

[Fin06] Kevin M. Finnigin. Cryptanalysis of pseudorandom number generators in wireless sensor networks. Master's thesis, Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson AFB, OH, USA, 2006.

FIPS:2000:DSS

[FIP00] FIPS. *Digital Signature Standard (DSS)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 27, 2000. ii + 74 pp. URL http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf.

FIPS:2001:AES

[FIP01a] FIPS. *Advanced Encryption Standard (AES)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, November 26, 2001. iv + 47 pp. URL http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

FIPS:2001:SRC

[FIP01b] FIPS. *Security Requirements for Cryptographic Modules*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, May 25, 2001. viii + 61 pp. URL http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf; http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf; http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf; http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf; http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf. Annex A: Approved Security Functions (19 May 2005); Annex B: Approved Protection Profiles (04 November 2004); Annex C: Approved Random Number Generators (31 January 2005); Annex D: Approved Key Establishment Techniques (30 June 2005). Supersedes FIPS PUB 140-1, 1994 January 11.

FIPS:2002:KHM

[FIP02a] FIPS. *The Keyed-Hash Message Authentication Code (HMAC)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, March 6, 2002. vii + 13 pp. URL http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf.

FIPS:2002:SHS

[FIP02b] FIPS. *Secure Hash Standard*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, August 1, 2002. iv + 79 pp. URL http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf.

Freedman:2005:KSO

[FIPR05] Michael J. Freedman, Yuval Ishai, Benny Pinkas, and Omer Reingold. Keyword search and oblivious pseudorandom functions. In Kilian [Kil05], pages 303–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Fischlin:2001:CLP

[Fis01a] Marc Fischlin. Cryptographic limitations on parallelizing membership and equivalence queries with applications to random-self-reductions. *Theoretical Computer Science*, 268(2):199–219, October 17, 2001. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.nl/gej-ng/10/41/16/217/31/29/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/217/31/29/article.pdf.

Fischlin:2001:ICN

[Fis01b] Marc Fischlin. On the impossibility of constructing non-interactive statistically-secret protocols from any trapdoor one-way function. *Lecture Notes in Computer Science*, 2271:79–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710079.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710079.pdf.

Fischlin:2005:CEN

[Fis05] Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In Shoup [Sho05a], pages 152–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Faugere:2003:ACH

[FJ03] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. In Boneh [Bon03], pages 44–60. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Feng:2004:PEX

[FJ04] L. Feng and W. Jonker. Preparations for encrypted XML metadata querying. *International Journal of Computer Systems Science and Engineering*, 19(3): ??, May 2004. CODEN CSSEEI. ISSN 0267-6192.

Ferguson:2001:ICRb

[FKL+01a] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting. Improved cryptanalysis of Rijndael. In Schneier [Sch01d], pages 19–?? CODEN LNCSD9. ISBN 3-540-41728-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no. 1978. URL http://www.counterpane.com/rijndael.html; http://www.counterpane.com/rijndael.ps.zip.

Ferguson:2001:ICRa

[FKL+01b] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. *Lecture Notes in Computer Science*, 1978: 213–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780213.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780213.pdf.

Ferguson:2000:ICR

[FKS+00] Niels Ferguson, John Kelsey, Bruce Schneier, Mike Stay, David Wagner, and Doug

Whiting. Improved cryptanalysis of Rijndael (abstract only). In NIST [NIS00], page 9. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Ferguson:2000:TRR

[FKSW00] N. Ferguson, J. Kelsey, B. Schneier, and D. Wagner. A Twofish retreat: Related-key attacks against reduced-round Twofish. Twofish technical report 6, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, February 14, 2000. ???? pp.

Fluhrer:2001:AES

[FL01a] Scott Fluhrer and Stefan Lucks. Analysis of the E_0 encryption system. *Lecture Notes in Computer Science*, 2259:38–48, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590038.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590038.pdf.

Fox:2001:PPK

[FL01b] Barbara Fox and Brian LaMacchia. Panel: Public key infrastructure: PKIX, signed XML or something else? *Lecture Notes in Computer Science*, 1962: 327–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620327.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620327.pdf.

Faure:2006:NPK

[FL06] Cédric Faure and Pierre Loidreau. A new public-key cryptosystem based on the problem of reconstructing p-polynomials. In Ytrehus [Ytr06], pages 304–315. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Freytag:2003:VPI

[FLA+03] Johann Christoph Freytag, Peter C. Lockemann, Serge Abiteboul, Michael J. Carey, Patricia G. Selinger, and Andreas Heuer, editors. *VLDB 2003: Proceedings of 29th International Conference on Very Large Data Bases, September 9–12, 2003, Berlin, Germany*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 2003. ISBN 0-12-722442-4. LCCN ????

Fluhrer:2002:CMB

[Flu02a] Scott R. Fluhrer. Cryptanalysis of the mercy block cipher. *Lecture Notes in Computer Science*, 2355: 28–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550028.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550028.pdf`.

Fluhrer:2002:CSP

[Flu02b] Scott R. Fluhrer. Cryptanalysis of the SEAL 3.0 pseudorandom function family. *Lecture Notes in Computer Science*, 2355: 135–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550135.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550135.pdf`.

Feng:2006:ISC

[FLY06] Dengguo Feng, Dongdai Lin, and Moti Yung, editors. *Information Security and Cryptology: First SKLOIS Conference, CISC 2005, Beijing, China, December 15–17, 2005. Proceedings*, volume 3822 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-30855-5 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3822`.

Fan:2002:ETB

[FLZ02] Lei Fan, Jian-Hua Li, and Hong-Wen Zhu. An enhancement of timestamp-based password authentication scheme. *Computers & Security*, 21(7):665–667, November 2002. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404802011185`.

Fehr:2002:LVD

[FM02a] Serge Fehr and Ueli Maurer. Linear VSS and distributed commitments based on secret sharing and pairwise checks. In Yung [Yun02a], pages 565–580. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420565.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420565.pdf.

Fuller:2002:LRA

[FM02b] Joanne Fuller and William Millan. On linear redundancy in the AES S-box. Report 2002/111, Cryptology ePrint Archive, 2002. URL http://eprint.iacr.org/2002/111.ps; http://eprint.iacr.org/2002/111.ps.gz; http://eprint.iacr.org/2002/111/.

Franklin:2002:PAS

[FMA02] Michael Franklin, Bongki Moon, and Anastassia Ailamaki, editors. *Proceedings of the ACM SIGMOD International Conference on Management of Data, June 3–6, 2002, Madison, WI, USA*. ACM Press, New York, NY 10036, USA, 2002. ISBN ???? LCCN ???? ACM order number 475020.

Fournier:2003:SEA

[FML+03] Jacques J. A. Fournier, Simon Moore, Huiyun Li, Robert Mullins, and George Taylor. Security evaluation of asynchronous circuits. In Walter et al. [WKP03], pages 137–151. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Fouque:2003:AUR

[FMP03] Pierre-Alain Fouque, Gwenaëlle Martinet, and Guillaume Poupard. Attacking unbalanced RSA–CRT using SPA. In Walter et al. [WKP03], pages 254–268. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Fluhrer:2001:WKS

[FMS01] Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. In Serge Vaudenay and Amr M. Youssef, editors, *Selected areas in cryptography: 8th Annual International Workshop, SAC 2001, Toronto, Ontario, Canada, August 16–17, 2001: revised papers*, volume 2259 of *Lecture Notes in Computer Science*, pages 1–24. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-43066-0. LCCN QA76.9.A25 S22 2001. URL http://dl.acm.org/citation.cfm?id=694759; http://link.springer-ny.com/link/service/series/0558/tocs/t2259.htm; http://www.crypto.com/papers/others/rc4_ksaproc.pdf; http://www.loc.gov/catdir/enhancements/fy0817/2002511206-d.html.

Furht:2005:MEW

[FMS05] Borivoje (Borko) Furht, Edin Muharemagic, and Daniel Socek. *Multimedia encryption and watermarking*, volume 28 of *Multimedia systems and applications*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 0-387-24425-5; 0-387-26090-0. ???? pp. LCCN QA76.575 .F885 2005.

Frankel:2001:ASA

[FMY01] Yair Frankel, Philip D. MacKenzie, and Moti Yung. Adaptive security for the additive-sharing based proactive RSA. *Lecture Notes in Computer Science*, 1992: 240–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920240.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920240.pdf.

Frankel:2002:ASD

[FMY02] Yair Frankel, Philip MacKenzie, and Moti Yung. Adaptively secure distributed public-key systems. *Theoretical Computer Science*, 287(2):535–561, September 2002. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Fair:2005:CST

[FNRC05] Ted Fair, Michael Nordfelt, Sandra Ring, and Eric Cole. *Cyber spying: tracking your family's (sometimes) secret online lives*. Syngress Publishing, Inc., Rockland, MA, USA, 2005. xxiii + 439 pp. URL ftp://

uiarchive.cso.uiuc.edu/pub/etext/gutenberg/; http://site.ebrary.com/lib/ucsc/Doc?id=10074965.

Foster:2005:BOA

[FOBH05] James C. Foster, Vitaly Osipov, Nish Bhalla, and Niels Heinen, editors. *Buffer Overflow Attacks: Detect, Exploit, Prevent*. Syngress Publishing, Inc., Rockland, MA, USA, 2005. ISBN 1-932266-67-4. xxii + 497 pp. LCCN QA76.9.A25 B83 2005. Foreword by Dave Aitel.

Fricke:2006:ESI

[FOP06] D. Frincke, S. Oudekirk, and B. Popovsky. Editorial: Special issue on resources for the computer security and information assurance curriculum: Issue 1. *ACM Journal on Educational Resources in Computing (JERIC)*, 6(3):1:1–1:??, September 2006. CODEN ???? ISSN 1531-4278.

Fujisaki:2001:ROS

[FOPS01] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. RSA–OAEP is secure under the RSA assumption. In Kilian [Kil01a], pages 260–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390260.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390260.pdf.

Forbes:2004:BRN

[For04] Scott Forbes. Book reviews: *A .NET Gold Mine: .NET Security and Cryptography*, by Peter Thorsteinson and G. Gnana Arun Ganesh (Prentice-Hall 2004, ISBN 0-13-100851-X). *IEEE Security & Privacy*, 2(4): 10, July/August 2004. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://csdl.computer.org/dl/mags/sp/2004/04/j4010.htm.

Forte:2009:DM

[For09] Dario Forte. The death of MD5. *Network Security*, 2009(2):18–20, February 2009. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485809700200.

Fox:2000:NTFb

[Fox00] Robert Fox. News track: Flying the rails; logging online hours at work; top prize: embedded encryption; Digital Nose knows; walking again via chip implant; cellphone-free class; another node in the crowd. *Communications of the Association for Computing Machinery*, 43(5):9, May 2000. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/2000-43-5/p9-fox/.

Freking:2000:MMR

[FP00] W. L. Freking and K. K. Parhi. Modular multiplication in the residue number system with application to massively-parallel public-key cryptography systems. In *Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers, 2000*, volume 2, pages 1339–1343. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2000. CODEN ???? ISSN ????

Fouque:2001:TCS

[FP01] Pierre-Alain Fouque and David Pointcheval. Threshold cryptosystems secure against chosen-ciphertext attacks. *Lecture Notes in Computer Science*, 2248: 351–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480351.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480351.pdf.

Faugere:2009:EAD

[FP09] Jean-Charles Faugère and Ludovic Perret. An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. *Journal of Symbolic Computation*, 44(12):1676–1689, December 2009. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Fouque:2001:SDC

[FPS01] Pierre-Alain Fouque, Guillaume Poupard, and Jacques Stern. Sharing decryption in the context of voting or lotteries. *Lecture Notes in Computer Science*, 1962:90–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620090.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620090.pdf.

Fernandes:2002:SAL

[FR02] Savio Fernandes and KLM Reddy. Securing applications on Linux with PAM. *Linux Journal*, 102:??, October 2002. CODEN LI-

JOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://www.linuxjournal.com/article.php?sid=5940.

Fournet:2008:CSI

[FR08] Cédric Fournet and Tamara Rezk. Cryptographically sound implementations for typed information-flow security. *ACM SIGPLAN Notices*, 43(1):323–335, January 2008. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Frankel:2001:FCI

[Fra01] Yair Frankel, editor. *Financial cryptography: 4th International Conference, FC 2000, Anguilla, British West Indies, February 20–24, 2000: Proceedings*, volume 1962 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-42700-7 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1962; HG1710 .F35 2000. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1962.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1962.

Franklin:2004:ACC

[Fra04] Matt Franklin, editor. *Advances in Cryptology — CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15–19, 2004. Proceedings*, volume 3152 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Fremberg:2003:MAP

[Fre03] Daniel Fremberg. The Mithra authentication protocol. *Dr. Dobb's Journal of Software Tools*, 28 (5):44, 46–48, May 2003. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/documents/s=7927/ddj0305d/.

Friberg:2001:UCH

[Fri01] Paul Friberg. Using a cryptographic hardware token with Linux: The OpenSSL project's new engine. *Linux Journal*, 89:??, September 2001. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://www.linuxjournal.com/articles/style/0006.html. Web only.

Frith:2007:SAO

[Fri07] David Frith. Steganography approaches, options, and implications. *Network Security*, 2007(8):4–7, August 2007. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485807700715.

Frykholm:2000:CAB

[Fry00] Niklas Frykholm. Countermeasures against buffer overflow attacks. Technical report, RSA Data Security, Inc., Redwood City, CA, USA, November 30, 2000. URL http://www.rsasecurity.com/rsalabs/technotes/buffer/buffer_overflow.html.

Ferguson:2000:CEI

[FS00] N. Ferguson and B. Schneier. A cryptographic evaluation of IPsec. Technical report, Counterpane Internet Security, 3031 Tisch Way, Suite 100PE, San Jose, CA 95128, USA, 2000. URL http://www.counterpane.com/ipsec.html; http://www.counterpane.com/ipsec.pdf.

Fouque:2001:FDT

[FS01a] Pierre-Alain Fouque and Jacques Stern. Fully distributed threshold RSA under standard assumptions. *Lecture Notes in Computer Science*, 2248: 310–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480310.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480310.pdf.

Friedlander:2001:DDH

[FS01b] John B. Friedlander and Igor E. Shparlinski. On the distribution of Diffie–Hellman triples with sparse exponents. *SIAM Journal on Discrete Mathematics*, 14 (2):162–169, 2001. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/36174.

Furukawa:2001:ESP

[FS01c] Jun Furukawa and Kazue Sako. An efficient scheme for proving a shuffle. In Kilian [Kil01a], pages 368–

?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390368.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390368.pdf.

Fischer:2002:NFC

[FS02] Wieland Fischer and Jean-Pierre Seifert. Note on fast computation of secret RSA exponents. *Lecture Notes in Computer Science*, 2384:136–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840136.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840136.pdf.

Ferguson:2003:CEI

[FS03a] Niels Ferguson and Bruce Schneier. A cryptographic evaluation of IPsec. Unknown, 2003. URL https://www.schneier.com/paper-ipsec.html.

Ferguson:2003:PC

[FS03b] Niels Ferguson and Bruce Schneier. *Practical Cryptography*. John Wiley and Sons, Inc., New York, NY, USA, 2003. ISBN 0-471-22894-X (hardcover), 0-471-22357-3 (paperback). xx + 410 pp. LCCN QA76.9.A25 F466 2003. URL http://www.counterpane.com/book-practical.html; http://www.loc.gov/catdir/bios/wiley044/2003276249.html; http://www.loc.gov/catdir/description/wiley036/2003276249.html; http://www.loc.gov/catdir/toc/wiley032/2003276249.html.

Fundulaki:2004:SYD

[FS04] Irini Fundulaki and Arnaud Sahuguet. "share your data, keep your secrets". In ACM [ACM04a], pages 945–946. ISBN 1-58113-859-8. LCCN QA76.9.D3.

Fortnow:2008:IIC

[FS08] Lance Fortnow and Rahul Santhanam. Infeasibility of instance compression and succinct PCPs for NP. In ACM [ACM08], pages 133–142. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Fuster-Sabater:2001:EAG

[FSGV01] A. Fúster-Sabater and L. J. García-Villalba. An efficient algorithm to generate binary sequences for cryptographic purposes. *Theoretical Computer Science*, 259(1–2):679–688, May 28, 2001. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.nl/gej-ng/10/41/16/202/21/54/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/202/21/54/article.pdf.

Fu:2001:DCA

[FSSF01] Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. The dos and don'ts of client authentication on the Web. In USENIX [USE01c], page ?? ISBN 1-880446-18-9, 1-880446-07-3. LCCN QA76.9.A25 U565 2001. URL http://www.usenix.org/publications/library/proceedings/sec01/fu.html.

Ferguson:2001:SAR

[FSW01] Niels Ferguson, Richard Schroeppel, and Doug Whiting. A simple algebraic representation of Rijndael. *Lecture Notes in Computer Science*, 2259: 103–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590103.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590103.pdf.

Furman:2001:CSM

[Fur01] Vladimir Furman. Cryptanalysis of some modern blockciphers. Thesis (Master's), Faculty of Computer Science, Technion — Israel Institute of Technology, Haifa, Israel, 2001. 75 pp.

Furman:2002:DCN

[Fur02a] Vladimir Furman. Differential cryptanalysis of Nimbus. *Lecture Notes in Computer Science*, 2355: 187–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550187.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550187.pdf.

Furuya:2002:SAK

[Fur02b] Soichi Furuya. Slide attacks with a known-plaintext cryptanalysis. *Lecture Notes in Computer Science*, 2288: 214–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880214.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880214.pdf.

Furnell:2005:AOW

[Fur05] Steven Furnell. Authenticating ourselves: will we ever escape the password? *Network Security*, 2005(3): 8–13, March 2005. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485805002126.

Fouque:2003:DAW

[FV03] Pierre-Alain Fouque and Frederic Valette. The doubling attack — why upwards is better than downwards. In Walter et al. [WKP03], pages 269–280. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Feldhofer:2009:HIS

[FW09] Martin Feldhofer and Johannes Wolkerstorfer. Hardware implementation of symmetric algorithms for RFID security. In Paris Kitsos and Yan Zhang, editors, *RFID Security: Techniques, Protocols and System-on-Chip Design*, pages 373–415. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 0-387-76481-X (e-book), 0-387-76480-1 (hardcover). LCCN TK6553 .R45 2008eb. URL http://www.springerlink.com/content/q1160h1036371331/.

Fan:2008:RSB

[FWL08] Ming-Quan Fan, Hong-Xia Wang, and Sheng-Kun Li. Restudy on SVD-based watermarking scheme. *Applied Mathematics and Computation*, 203(2):926–930, September 15, 2008. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Feng:2005:NMS

[FWTC05] Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, and Yen-Ping Chu. A new multi-secret images sharing scheme using Lagrange's interpolation. *The Journal of Systems and Software*, 76(3):327–339, June 2005. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Fitzi:2004:PSB

[FWW04] Matthias Fitzi, Stefan Wolf, and Jürg Wullschleger. Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. In Franklin [Fra04], pages 562–?? CO-

DEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Fan:2004:PPI

[FXAM04] Jinliang Fan, Jun Xu, Mostafa H. Ammar, and Sue B. Moon. Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme. *Computer Networks (Amsterdam, Netherlands: 1999)*, 46(2):253–272, October 7, 2004. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Furnell:2006:RPS

[FZ06] Steven Furnell and Leith Zekri. Replacing passwords: in search of the secret remedy. *Network Security*, 2006 (1):4–8, January 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348580670321X.

Fu:2005:DHP

[FZH05] Yongzhi Fu, Xuejie Zhang, and Lin Hao. Design of high performance reconfigurable Triple DES processor. In Han et al. [HYZ05b], pages 110–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Gross-Amblard:2003:QPW

[GA03] David Gross-Amblard. Query-preserving watermarking of relational databases and XML documents. In ACM [ACM03c], pages 191–201. ISBN 1-58113-670-6. LCCN QA76.9.D3 A296 2003. ACM order number 475030.

Gang:2005:CNI

[GA05] Litao Gang and Ali N. Akansu. Cover noise interference suppression in multimedia data hiding. *International Journal of Image and Graphics (IJIG)*, 5(1):191–??, January 2005. CODEN ???? ISSN 0219-4678.

Galbraith:2001:SCC

[Gal01] Steven D. Galbraith. Supersingular curves in cryptography. *Lecture Notes in Computer Science*, 2248:495–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480495.htm; http://link.springer-

ny.com/link/service/series/0558/papers/2248/22480495.pdf.

Galbreath:2002:CID

[Gal02] Nicholas Galbreath. *Cryptography for Internet and database applications: developing secret and public key techniques with Java*. John Wiley and Sons, Inc., New York, NY, USA, 2002. ISBN 0-471-21029-3. 400 pp. LCCN QA76.9.A25 G35 2002.

Gallo:2003:SST

[Gal03] Vince Gallo. Secret steganography techniques revealed. *Network Security*, 2003(2):4–8, February 2003. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485803002095.

Ganger:2001:AC

[Gan01a] G. R. Ganger. Authentication confidences. In IEEE [IEE01b], page 169. ISBN 0-7695-1040-X. US$135.00. URL http://computer.org/CSPRESS/CATALOG/pr01040.htm. IEEE catalog number PR01040.

Gannon:2001:SST

[Gan01b] James Gannon. *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*. Brassey's, Washington, DC, USA, 2001. ISBN 1-57488-367-4, 1-57488-473-5, 1-61234-207-8. xi + 324 pp. LCCN JF 1525 .I6G36 2001X ROBA; JF1525.I6 G36 2001.

Ganti:2008:PAL

[Gan08] Ashwin Ganti. Plan 9 authentication in Linux. *Operating Systems Review*, 42 (5):27–33, July 2008. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Garrett:2001:MBC

[Gar01] Paul B. Garrett. *Making, breaking codes: an introduction to cryptology*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 2001. ISBN 0-13-030369-0. xix + 524 pp. LCCN QA268 .G37 2001.

Garfinkel:2003:EBI

[Gar03a] Simson L. Garfinkel. Email-based identification and authentication: An alternative to PKI? *IEEE Security & Privacy*, 1(6):20–26, November/December 2003. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://csdl.computer.org/comp/mags/sp/2003/06/j6020abs.htm; http://csdl.computer.org/dl/mags/sp/2003/06/j6020.htm; http://csdl.computer.org/dl/mags/sp/2003/06/j6020.pdf.

Garman:2003:KDG

[Gar03b] Jason Garman. *Kerberos: the definitive guide*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, 2003. ISBN 0-596-00403-6. xiv + 253 pp. LCCN TK5105.59 .G375 2003. URL `http://www.oreilly.com/catalog/9780596004033`.

Garrett:2004:MCT

[Gar04] Paul B. Garrett. *The mathematics of coding theory: information, compression, error correction, and finite fields*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 2004. ISBN 0-13-101967-8. x + 398 pp. LCCN QA275 .G26 2003.

Garrett:2005:CP

[Gar05] Paul Garrett. Cryptographic primitives. In Garrett and Lieman [GL05], pages 1–62. ISBN 0-8218-3365-0. LCCN QA76.9.A25 P82 2005. URL `http://www.loc.gov/catdir/toc/fy0612/2005048178.html`.

Gasarch:2001:BRBa

[Gas01] William Gasarch. Book review: *The Codebreakers: the Story of Secret Writing*, by David Kahn. Scribner. *ACM SIGACT News*, 32(2):5–6, June 2001. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Kah67a, Kah67b, Kah74, Kah96].

Gaudry:2002:CCS

[Gau02] Pierrick Gaudry. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. *Lecture Notes in Computer Science*, 2501: 311–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2501/25010311.htm`; `http://link.springer.de/link/service/series/0558/papers/2501/25010311.pdf`.

Gavinsky:2008:CIC

[Gav08] Dmitry Gavinsky. Classical interaction cannot replace a quantum message. In ACM [ACM08], pages 95–102. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Guinee:2009:NTR

[GB09] R. A. Guinee and M. Blaszczyk. A novel true random binary sequence generator based on a chaotic double scroll oscillator combination with a pseudo random generator for cryptographic applications. In *ICITST 2009. International Con-*

ference for Internet Technology and Secured Transactions, 2009*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5402536.

Guajardo:2001:EIE

[GBKP01] Jorge Guajardo, Rainer Blümel, Uwe Krieger, and Christof Paar. Efficient implementation of elliptic curve cryptosystems on the TI MSP430x33x family of microcontrollers. *Lecture Notes in Computer Science*, 1992:365–382, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Golic:2002:LCB

[GBM02] Jovan Dj. Golić, Vittorio Bagini, and Guglielmo Morgari. Linear cryptanalysis of Bluetooth stream cipher. *Lecture Notes in Computer Science*, 2332: 238–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320238.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320238.pdf.

Gaj:2000:CHP

[GC00a] Kris Gaj and Pawel Chodowiec. Comparison of the hardware performance of the AES candidates using reconfigurable hardware. In NIST [NIS00], pages 40–56. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Goubin:2000:CTC

[GC00b] Louis Goubin and Nicolas T. Courtois. Cryptanalysis of the TTM cryptosystem. *Lecture Notes in Computer Science*, 1976:44–57, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gaj:2001:FIF

[GC01a] Kris Gaj and Pawel Chodowiec. Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using field programmable gate arrays. In *Topics in* *cryptology—CT-RSA 2001 (San Francisco, CA)*, volume 2020 of *Lecture Notes in Comput. Sci.*, pages 84–99. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200084.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200084.pdf`.

Goodman:2001:EER

[GC01b] James Goodman and Anantha Chandrakasan. An energy efficient reconfigurable public-key cryptography processor architecture. *Lecture Notes in Computer Science*, 1965: 175–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650175.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650175.pdf`.

Guerrero:2005:ECB

[GC05] Jorge Herrerías Guerrero and Roberto Gómez Cárdenas. An example of communication between security tools: IPTables — Snort. *Operating Systems Review*, 39(3): 34–43, July 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Gordon:2008:CFS

[GCKL08] Dov S. Gordon, Hazay Carmit, Jonathan Katz, and Yehuda Lindell. Complete fairness in secure two-party computation. In ACM [ACM08], pages 413–422. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Gligor:2002:FEA

[GD02] Virgil D. Gligor and Pompiliu Donescu. Fast encryption and authentication: XCBC encryption and XECB authentication modes. *Lecture Notes in Computer Science*, 2355: 92–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550092.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550092.pdf`.

Gennaro:2005:SMS

[GD05] Rosario Gennaro and Mario Di Raimondo. Secure multiplication of shared secrets in the exponent. *Information Processing Letters*, 96 (2):71–79, October 31, 2005. CODEN IFPLAT. ISSN

0020-0190 (print), 1872-6119 (electronic).

Gebotys:2004:DSC

[Geb04] Catherine H. Gebotys. Design of secure cryptography against the threat of power-attacks in DSP-embedded processors. *ACM Transactions on Embedded Computing Systems*, 3(1):92–113, February 2004. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Geier:2003:LCC

[Gei03] M. J. Geier. Lights, camera, controls! [dvd copying prevention]. *IEEE Spectrum*, 40 (5):28–31, May 2003. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Gengler:2000:UPC

[Gen00a] Barbara Gengler. US President Clinton signs Digital Signature Bill. *Network Security*, 2000(9):7–8, September 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485800090231`.

Gennaro:2000:IPR

[Gen00b] Rosario Gennaro. An improved pseudo-random generator based on discrete log. In Bellare [Bel00], pages 469–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800469.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1880/18800469.pdf`.

Gengler:2001:PPS

[Gen01] Barbara Gengler. Princeton poll shows 56% favour crypto regulations. *Network Security*, 2001(11):5–6, November 30, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485801011126`.

Gentry:2003:CBE

[Gen03] Craig Gentry. Certificate-based encryption and the certificate revocation problem. *Lecture Notes in Computer Science*, 2656: 272–293, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/3-540-39200-9_17.pdf`.

Gennaro:2004:MTC

[Gen04a] Rosario Gennaro. Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks. In Franklin [Fra04], pages 220–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Gentry:2004:HCR

[Gen04b] Craig Gentry. How to compress Rabin ciphertexts and signatures (and more). In Franklin [Fra04], pages 179–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Gennaro:2006:RC

[Gen06] Rosario Gennaro. Randomness in cryptography. *IEEE Security & Privacy*, 4(2):64–67, March/April 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Gentry:2009:FHEa

[Gen09a] Craig Gentry. *A fully homomorphic encryption scheme*. Ph.d. thesis, Department of Computer Science, Stanford University, Stanford, CA, USA, 2009. x + 199 pp. URL http://crypto.stanford.edu/craig/; http://crypto.stanford.edu/craig/craig-thesis.pdf.

Gentry:2009:FHEb

[Gen09b] Craig Gentry. Fully homomorphic encryption using ideal lattices. In ACM [ACM09], pages 169–178. ISBN 1-60558-613-7. LCCN QA75.5 .A22 2009.

Giuliani:2001:GLI

[GG01] Kenneth J. Giuliani and Guang Gong. Generating large instances of the Gong–Harn cryptosystem. *Lecture Notes in Computer Science*, 2260:317–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600317.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600317.pdf.

Goldstone:2005:FCR

[GG05a] Lawrence Goldstone and Nancy Bazelon Goldstone.

The Friar and the Cipher: Roger Bacon and the Unsolved Mystery of the Most Unusual Manuscript in the World. Doubleday, New York, NY, USA, 2005. ISBN 0-7679-1473-2. xi + 320 pp. LCCN Z105.5.V65 G65 2005. URL http://www.loc.gov/catdir/bios/random056/2004050164.html; http://www.loc.gov/catdir/description/random051/2004050164.html; http://www.loc.gov/catdir/enhancements/fy0618/2004050164-s.html.

Golomb:2005:SDG

[GG05b] Solomon W. (Solomon Wolf) Golomb and Guang Gong. *Signal design for good correlation for wireless communication, cryptography, and radar*. Cambridge University Press, Cambridge, UK, 2005. ISBN 0-521-82104-5 (hardcover). xviii + 438 pp. LCCN TK5102.92 .G65 2005. URL http://www.loc.gov/catdir/toc/ecip057/2005002719.html.

Gambino:2008:ITW

[GG08] Nicola Gambino and Richard Garner. The identity type weak factorisation system. *Theoretical Computer Science*, 409(1):94–109, December 6, 2008. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Goldwasser:2008:CAP

[GGH+08] Shafi Goldwasser, Dan Gutfreund, Alexander Healy, Tali Kaufman, and Guy N. Rothblum. A (de)constructive approach to program checking. In ACM [ACM08], pages 143–152. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Gennaro:2003:LBE

[GGK03] Rosario Gennaro, Yael Gertner, and Jonathan Katz. Lower bounds on the efficiency of encryption and digital signature schemes. In ACM [ACM03b], pages 417–425. ISBN ???? LCCN QA75.5 .A22 2003. ACM order number 508030.

Gennaro:2005:BEG

[GGKT05] Rosario Gennaro, Yael Gertner, Jonathan Katz, and Luca Trevisan. Bounds on the efficiency of generic cryptographic constructions. *SIAM Journal on Computing*, 35(1):217–246, ???? 2005. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Grothoff:2009:TBS

[GGS+09] Christian Grothoff, Krista Grothoff, Ryan Stutsman, Ludmila Alkhutova, and Mikhail Atallah. Translation-based steganography. *Journal of Computer Security*, 17(3):269–303, ???? 2009. CODEN JCSIET. ISSN

0926-227X (print), 1875-8924 (electronic).

Gilbert:2002:SCL

[GH02] Gerald Gilbert and Michael Hamrick. Secrecy, computational loads and rates in practical quantum cryptography. *Algorithmica*, 34(4):314–339, November 2002. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=34&issue=4&spage=314. Quantum computation and quantum cryptography.

Gross:2004:MNh

[GH04] Benedict H. Gross and Joe Harris. *The Magic of Numbers*. Pearson Education, Upper Saddle River, NJ, USA, 2004. ISBN 0-13-177721-1. xiv + 287 pp. LCCN QA39.3 .G76 2003.

Gilbert:2005:FSE

[GH05] Henri Gilbert and Helena Handschuh, editors. *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21–23, 2005, Revised Selected Papers*, volume 3557 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-26541-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F77 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3557.

Galindo:2008:SPK

[GH08] David Galindo and Javier Herranz. On the security of public key cryptosystems with a double decryption mechanism. *Information Processing Letters*, 108(5):279–283, November 15, 2008. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ghafarian:2007:IPU

[Gha07] Ahmad Ghafarian. Ideas for projects in undergraduate information assurance and security courses. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 39(3):322, September 2007. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). Proceedings of the 12th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education (ITiCSE'07).

Gonzales:2000:LBC

[GHdGSS00] Octavio A. Gonzales, Gunhee Han, José Pineda de Gyvez, and Edgar Sánchez-Sinencio. Lorenz-based chaotic cryptosystem: a monolithic implementation. *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, 47(8):1243–1247, 2000. CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic).

Gilbert:2000:SAR

[GHJV00] Henri Gilbert, Helena Handschuh, Antoine Joux, and Serge Vaudenay. A statistical attack on RC6 (abstract only). In NIST [NIS00], page 10. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Gilbert:2001:SAR

[GHJV01] H. Gilbert, H. Handschuh, A. Joux, and Serge Vaudenay. A statistical attack on RC6. In Schneier [Sch01d], page ?? CODEN LNCSD9. ISBN 3-540-41728-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no. 1978. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1978.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1978.

Gaudry:2006:ACM

[GHK+06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. *Lecture Notes in Computer Science*, 4284:114–129, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11935230_8.pdf.

Grabner:2005:ALC

[GHPT05] Peter J. Grabner, Clemens Heuberger, Helmut Prodinger, and Jörg M. Thuswaldner. Analysis of linear combination algorithms in cryptography. *ACM Transactions on Algorithms*, 1(1):123–142, July 2005. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Gong:2001:GPK

[GHW01] Guang Gong, Lein Harn,

and Huapeng Wu. The GH public-key cryptosystem. *Lecture Notes in Computer Science*, 2259: 284–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590284.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590284.pdf.

Gennaro:2001:RCV

[GIKR01] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. The round complexity of verifiable secret sharing and secure multicast. In ACM [ACM01a], pages 580–589. ISBN 1-58113-349-9. LCCN QA76.6 .A13 2001. ACM order number 508010.

Gennaro:2002:RSM

[GIKR02] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. On 2-round secure multiparty computation. In Yung [Yun02a], pages 178–193. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Gillespie:2007:WSC

[Gil07] Tarleton Gillespie. *Wired shut: copyright and the shape of digital culture*. MIT Press, Cambridge, MA, USA, 2007. ISBN 0-262-07282-3. 420 (est.) pp. LCCN K1447.15 .G55 2007. URL http://www.loc.gov/catdir/toc/ecip0620/2006030129.html.

Giraud:2006:RIR

[Gir06] C. Giraud. An RSA implementation resistant to fault attacks and to simple power analysis. *IEEE Transactions on Computers*, 55(9): 1116–1120, September 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1668039.

Gebhardt:2005:NPV

[GIS05] M. Gebhardt, G. Illies, and W. Schindler. A note on the practical value of single hash function collisions for special file formats. In *NIST Cryptographic Hash Workshop 2005*, page ?? ????, ????, 2005. ISBN ???? LCCN ???? URL http://csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Illies_

NIST_05.pdf. 18 slides + 15-page paper.

Gordon:2003:ATS

[GJ03] Andrew D. Gordon and Alan Jeffrey. Authenticity by typing for security protocols. *Journal of Computer Security*, 11 (4):451–519, ???? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gordon:2004:TEA

[GJ04] Andrew D. Gordon and Alan Jeffrey. Types and effects for asymmetric cryptographic protocols. *Journal of Computer Security*, 12(3–4):435–483, ???? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ganapathy:2005:APA

[GJJ05] Vinod Ganapathy, Trent Jaeger, and Somesh Jha. Automatic placement of authorization hooks in the Linux security modules framework. In Meadows and Syverson [MS05b], pages 330–339. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Gennaro:2003:SAP

[GJKR03] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Secure applications of Pedersen's distributed key generation protocol. In Joye [Joy03b], pages 373–390. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Gallagher:2006:HSB

[GJL06] Tom Gallagher, Bryan Jeffries, and Lawrence Landauer. *Hunting security bugs*. Secure software development series. Microsoft Press, Redmond, WA, USA, 2006. ISBN 0-7356-2187-X. xxv + 559 pp. LCCN QA76.9.A25 G356 2006.

Gentry:2001:CNS

[GJSS01] Craig Gentry, Jakob Jonsson, Jacques Stern, and Michael Szydlo. Cryptanalysis of the NTRU Signature Scheme (NSS) from Eurocrypt 2001. *Lecture Notes in Computer Science*, 2248:1–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480001.htm; http://link.springer-ny.com/link/service/series/

0558/papers/2248/22480001.pdf.

Gomulkiewicz:2002:HWA

[GK02] Marcin Gomułkiewicz and Mirosław Kutyłowski. Hamming weight attacks on cryptographic hardware — breaking masking defense. *Lecture Notes in Computer Science*, 2502:90–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2502/25020090.htm; http://link.springer.de/link/service/series/0558/papers/2502/25020090.pdf.

Goldsmith:2004:CAI

[GK04] Clair W. Goldsmith and Rob Kolstad. A conversation about identity management. *;login: the USENIX Association newsletter*, 29 (5):??, October 2004. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/2004-10/pdfs/interview.pdf.

Goldwasser:2005:PPK

[GK05] Shafi Goldwasser and Dmitriy Kharchenko. Proof of plaintext knowledge for the Ajtai–Dwork cryptosystem. In Kilian [Kil05], pages 529–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Gavinsky:2007:ESO

[GKK+07] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In ACM [ACM07], pages 516–525. ISBN 1-59593-631-9. LCCN QA75.5 .A22 2007.

Gavinsky:2009:ESO

[GKK+09] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM Journal on Computing*, 38(5):1695–1708, ???? 2009. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Garay:2007:RCA

[GKKO07] J. A. Garay, J. Katz, Chiu-Yuen Koo, and R. Ostrovsky. Round complexity of authenticated broadcast with a dishonest majority. In IEEE [IEE07], pages 658–668. ISBN 0-7695-3010-9. ISSN 0272-5428. LCCN QA76 .S974 2007. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4389466. IEEE Computer Society order number P3010.

Gertner:2000:RBP

[GKM+00] Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan. The relationship between public key encryption and oblivious transfer. In IEEE [IEE00a], pages 325–335. CODEN ASFPDV. ISBN 0-7695-0850-2, 0-7695-0851-0 (case), 0-7695-0852-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 2000. IEEE Computer Society order number PR00850.

Guneysu:2008:CC

[GKN+08] T. Guneysu, T. Kasper, M. Novotny, C. Paar, and A. Rupp. Cryptanalysis with COPACOBANA. *IEEE Transactions on Computers*, 57(11):1498–1513, November 2008. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4515858.

Gorodetsky:2005:CNS

[GKS05] Vladimir Gorodetsky, Igor Kotenko, and Victor Skormin, editors. *Computer network security: third international workshop on mathematical methods, models, and architectures for computer network security, MMM-ACNS 2005, St. Petersburg, Russia, September 24–28, 2005, proceedings*, volume 3685 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-29113-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ????

Goubault-Larrecq:2000:MAC

[GL00] Jean Goubault-Larrecq. A method for automatic cryptographic protocol verification. *Lecture Notes in Computer Science*, 1800: 977–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1800/18000977.htm; http://link.springer-ny.com/link/service/series/0558/papers/1800/18000977.pdf.

Goldreich:2001:SKG

[GL01] Oded Goldreich and Yehuda

Lindell. Session-key generation using human passwords only. In Kilian [Kil01a], pages 408–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390408.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390408.pdf.

Gennaro:2003:FPB

[GL03] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. *Lecture Notes in Computer Science*, 2656:524–543, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_33.pdf.

Garrett:2005:PKC

[GL05] Paul Garrett and Daniel Lieman, editors. *Public-key cryptography: American Mathematical Society short course, January 13–14, 2003, Baltimore, Maryland*, volume 62 of *Proceedings of symposia in applied mathematics [AMS short course lecture notes]*. American Mathematical Society, Providence, RI, USA, 2005. ISBN 0-8218-3365-0. LCCN QA76.9.A25 P82 2005. URL http://www.loc.gov/catdir/toc/fy0612/2005048178.html.

Gennaro:2006:FPB

[GL06a] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. *ACM Transactions on Information and System Security*, 9(2):181–234, May 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Goshi:2006:ADM

[GL06b] Justin Goshi and Richard E. Ladner. Algorithms for dynamic multicast key distribution. *ACM Journal of Experimental Algorithmics*, 11:1.4:1–1.4:??, ???? 2006. CODEN ???? ISSN 1084-6654.

Gassend:2004:IAI

[GLC+04] Blaise Gassend, Daihyun Lim, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. Identification and authentication of integrated circuits. *Concurrency and Computation: Practice and Experience*, 16(11):1077–1098, September 2004. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Grembowski:2002:CAH

[GLG+02] Tim Grembowski, Roar Lien, Kris Gaj, Nghi Nguyen, Peter Bellows, Jaroslav Flidr, Tom Lehman, and Brian Schott. Comparative analysis of the hardware implementations of hash functions SHA-1 and SHA-512. *Lecture Notes in Computer Science*, 2433:75–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330075.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2433/24330075.pdf`.

Gallant:2001:FPM

[GLV01] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In Kilian [Kil01a], pages 190–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390190.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2139/21390190.pdf`.

Gilbert:2000:CAR

[GM00a] Henri Gilbert and Marine Minier. A collision attack on 7 rounds of Rijndael. In NIST [NIS00], pages 230–241. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf`.

Girault:2000:CCP

[GM00b] Marc Girault and Jean-François Misarsky. Cryptanalysis of countermeasures proposed for repairing ISO 9796-1. *Lecture Notes in Computer Science*, 1807:81–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070081.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1807/18070081.pdf`.

Gennaro:2002:CPG

[GM02a] Rosario Gennaro and Daniele Micciancio. Cryptanalysis of a pseudorandom generator based on braid groups. *Lecture Notes in Computer Science*, 2332:1–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320001.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320001.pdf.

Gilbert:2002:CS

[GM02b] Henri Gilbert and Marine Minier. Cryptanalysis of SFLASH. *Lecture Notes in Computer Science*, 2332:288–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320288.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320288.pdf.

Gilbert:2002:NRP

[GM02c] Henri Gilbert and Marine Minier. New results on the pseudorandomness of some blockcipher constructions. *Lecture Notes in Computer Science*, 2355:248–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550248.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550248.pdf.

Galbraith:2003:IAU

[GM03] Steven D. Galbraith and Wenbo Mao. Invisibility and anonymity of undeniable and confirmer signatures. In Joye [Joy03b], pages 80–97. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Gorrieri:2004:SFR

[GM04] Roberto Gorrieri and Fabio Martinelli. A simple framework for real-time cryptographic protocol analysis with compositional proof rules. *Science of Computer Programming*, 50(1–3):23–49, March 2004. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic).

Giuliano:2000:ISC

[GMG00] Genevieve Giuliano, James E. Moore II, and Jacqueline Golob. Integrated smart-card fare system: results from field operational test. *Transportation research record*, pages 138–146, No 2000.

Galbraith:2002:PKS

[GMLS02] S. Galbraith, J. Malone-Lee, and N. P. Smart. Public key signatures in the multi-user setting. *Information Processing Letters*, 83(5):263–266, September 15, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Goots:2001:FEA

[GMM01] Nick D. Goots, Alexander A. Moldovyan, and Nick A. Moldovyan. Fast encryption algorithm Spectr-H64. *Lecture Notes in Computer Science*, 2052: 275–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2052/20520275.htm; http://link.springer-ny.com/link/service/series/0558/papers/2052/20520275.pdf.

Golle:2008:DCS

[GMM08] Philippe Golle, Frank McSherry, and Ilya Mironov. Data collection with self-enforcing privacy. *ACM Transactions on Information and System Security*, 12(2):9:1–9:??, December 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Galbraith:2001:CNR

[GMP01a] Steven D. Galbraith, Wenbo Mao, and Kenneth G. Paterson. A cautionary note regarding cryptographic protocols based on composite integers. Report HPL-2001-284, HP Laboratories Bristol, Bristol, UK, November 8, 2001. URL http://www.hpl.hp.com/techreports/2001/HPL-2001-284.html.

Galbraith:2001:RBU

[GMP01b] Steven D. Galbraith, Wenbo Mao, and Kenneth G. Paterson. RSA-based undeniable signatures for general moduli. *Lecture Notes in Computer Science*, 2271: 200–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710200.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710200.pdf.

Gentry:2005:PAK

[GMR05] Craig Gentry, Philip Mackenzie, and Zulfikar Ramzan. Password authenticated key exchange using hidden smooth subgroups. In Meadows and Syverson [MS05b], pages 299–309. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Galindo:2008:ICB

[GMR08] David Galindo, Paz Morillo, and Carla Ràfols. Improved certificate-based encryption in the standard model. *The Journal of Systems and Software*, 81 (7):1218–1226, July 2008. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Gopalakrishnan:2001:PWV

[GMV01] K. Gopalakrishnan, Nasir Memon, and Poorvi L. Vora. Protocols for watermark verification. *IEEE MultiMedia*, 8(4):66–70, October 2001. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://dlib.computer.org/mu/books/mu2001/pdf/u4066.pdf; http://www.computer.org/multimedia/mu2001/u4066abs.htm.

Grosek:2001:SPK

[GMW01] Otokar Grošek, Spyros S. Magliveras, and Wandi Wei. On the security of a public-key cryptosystem. In *Public-key cryptography and computational number theory (Warsaw, 2000)*, pages 71–75. Walter de Gruyter, New York, NY, USA, 2001.

Ge:2005:CCO

[GMW05] Gennian Ge, Ying Miao, and Lihua Wang. Combinatorial constructions for optimal splitting authentication codes. *SIAM Journal on Discrete Mathematics*, 18 (4):663–678, 2005. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/43546.

Gore:2001:CMT

[GN01] Rajeev Prabhakar Goré and Phuong Thê Nguyên. CardS4: Modal theorem proving on Java smartcards. *Lecture Notes in Computer Science*, 2140: 111–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400111.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400111.pdf.

Gratzer:2006:CLE

[GN06] Vanessa Gratzer and David Naccache. Cryptography, law enforcement, and mobile communications. *IEEE*

Security & Privacy, 4(6): 67–70, November/December 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Gutmann:2005:WHC

[GNP05] P. Gutmann, D. Naccache, and C. C. Palmer. When hashes collide [applied cryptography]. *IEEE Security & Privacy*, 3(3):68–71, May/June 2005. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://ieeexplore.ieee.org/iel5/8013/31002/01439506.pdf`; `http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=31002&arnumber=1439506&count=20&index=13`.

Gaj:2003:FME

[GO03] Kris Gaj and Arkadiusz Orłowski. Facts and myths of Enigma: Breaking stereotypes. *Lecture Notes in Computer Science*, 2656: 106–122, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/3-540-39200-9_7.pdf`.

Goldreich:1999:MCP

[Gol99] Oded Goldreich. *Modern cryptography, probabilistic proofs, and pseudorandomness*, volume 17 of *Algorithms and combinatorics, 0937-5511*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-64766-X. xv + 182 pp. LCCN QA76.9.A25 G64 1999. URL `http://www.loc.gov/catdir/enhancements/fy0815/98050548-d.html`; `http://www.loc.gov/catdir/enhancements/fy0815/98050548-t.html`.

Goldreich:2001:FCBb

[Gol01a] Oded Goldreich. *Foundations of Cryptography: Basic Applications*, volume 2. Cambridge University Press, Cambridge, UK, 2001. ISBN 0-521-83084-2 (hardcover). xii + 373–798 pp. LCCN QA268.G5745 2001. US$54.95 (hardcover). See also volume 2 [Gol04].

Goldreich:2001:FCBa

[Gol01b] Oded Goldreich. *Foundations of Cryptography: Basic Tools*, volume 1. Cambridge University Press, Cambridge, UK, 2001. ISBN 0-521-03536-8 (paperback), 0-521-79172-3 (hardcover). xix + 372 pp. LCCN QA268 .G5745 2001. US$54.95 (hardcover). See also volume 2 [Gol04].

Golic:2001:CAS

[Gol01c] Jovan D. Golić. Correlation analysis of the shrinking generator. In Kilian [Kil01a], pages 440–

?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390440.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390440.pdf.

Golic:2001:HCC

[Gol01d] Jovan Dj. Golić. How to construct cryptographic primitives from stream ciphers. *Computers & Security*, 20(1):79–89, January 31, 2001. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404801010252.

Golic:2001:MOS

[Gol01e] Jovan Dj. Golic. Modes of operation of stream ciphers. *Lecture Notes in Computer Science*, 2012: 233–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120233.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120233.pdf.

Golic:2003:DNP

[Gol03] Jovan D. Golić. DeKaRT: a new paradigm for key-dependent reversible circuits. In Walter et al. [WKP03], pages 98–112. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Goldreich:2004:FCV

[Gol04] Oded Goldreich. *Foundations of Cryptography: Volume 2: Basic Applications*. Cambridge University Press, Cambridge, UK, 2004. ISBN 0-521-83084-2. 373–798 pp. LCCN QA268 .G5745 2001. URL http://www.loc.gov/catdir/description/cam021/00049362.html; http://www.loc.gov/catdir/toc/cam023/00049362.html. See also volume 1 [Gol01b].

Goldstein:2008:BHO

[Gol08] Emmanuel Goldstein. *The best of 2600: a hacker odyssey*. John Wiley and Sons, Inc., New York, NY, USA, 2008. ISBN 0-470-

29419-1 (cloth). xvi + 871 pp. LCCN QA76.9.A25 G643 2008. URL http://www.loc.gov/catdir/enhancements/fy0833/2008018567-d.html; http://www.loc.gov/catdir/enhancements/fy0833/2008018567-t.html.

Gonda:2006:NMR

[Gon06] J. Gonda. The number of the modulo n roots of the polynomial x^v — x^v and the RSA. *J.UCS: Journal of Universal Computer Science*, 12(9):1215–1228, ???? 2006. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_12_9/the_number_of_the.

Good:2000:TAE

[Goo00] I. J. Good. Turing's anticipation of empirical Bayes in connection with the cryptanalysis of the naval Enigma. *Journal of Statistical Computation and Simulation*, 66(2):101–111, 2000. CODEN JSCSAT. ISSN 0094-9655 (print), 1563-5163 (electronic). 50th Anniversary of the Department of Statistics, Virginia Tech, Part II (Blacksburg, VA, 1999).

Gordon:2002:TCP

[Gor02a] Andrew D. Gordon. Types for cryptographic protocols. *Lecture Notes in Computer Science*, 2421: 99–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2421/24210099.htm; http://link.springer.de/link/service/series/0558/papers/2421/24210099.pdf.

Gurgens:2002:APF

[GOR02b] Sigrid Gürgens, Peter Ochsenschläger, and Carsten Rudolph. Authenticity and provability — A formal framework. *Lecture Notes in Computer Science*, 2437: 227–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2437/24370227.htm; http://link.springer.de/link/service/series/0558/papers/2437/24370227.pdf.

Gorman:2005:NSC

[Gor05] Sean P. Gorman. *Networks, security, and complexity: the role of public policy in critical infrastructure protection*. Edward Elgar Publishers, Northhampton, MA, USA, 2005. ISBN 1-84376-952-2. 153 (est.) pp. LCCN QA76.9.A25 G657 2005.

Gordon:2006:UAV

[Gor06] Sarah Gordon. Understanding the adversary: Virus writers and beyond. *IEEE*

Security & Privacy, 4(5): 67–70, September/October 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Goulding:2009:ESA

[Gou09] Tom Goulding. An encryption system in assembly language: a game-like project for novice programmers. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 41(4):40–44, December 2009. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Geppert:2000:TMS

[GP00] L. Geppert and Tekla S. Perry. Transmeta's magic show [microprocessor chips]. *IEEE Spectrum*, 37(5):26–33, May 2000. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Gupta:2008:FAT

[GPC08] Manish Gupta, Amit Pathak, and Soumen Chakrabarti. Fast algorithms for top-k personalized PageRank queries. In ACM, editor, *International World Wide Web Conference Proceeding of the 17th international conference on World Wide Web*, pages 1225–1226. ACM Press, New York, NY 10036, USA, 2008. ISBN 1-60558-085-6. LCCN ????

Ganeriwal:2008:STS

[GPČS08] Saurabh Ganeriwal, Christina Pöpper, Srdjan Čapkun, and Mani B. Srivastava. Secure time synchronization in sensor networks. *ACM Transactions on Information and System Security*, 11(4):23:1–23:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Garcia-Pasquel:2006:GCT

[GPG06] Jesús Adolfo García-Pasquel and José Galaviz. Ganzúa: a cryptanalysis tool for monoalphabetic and polyalphabetic ciphers. *ACM Journal on Educational Resources in Computing (JERIC)*, 6(3):4:1–4:??, September 2006. CODEN ???? ISSN 1531-4278.

Guneysu:2008:SPH

[GPP08] Tim Güneysu, Christof Paar, and Jan Pelzl. Special-purpose hardware for solving the elliptic curve discrete logarithm problem. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 1(2):8:1–8:??, June 2008. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Gutterman:2006:ALR

[GPR06] Zvi Gutterman, Benny Pinkas, and Tzachy Reinman. Analysis of the Linux random number generator. Report, The Hebrew University of Jerusalem and University of Haifa, Jerusalem and Haifa, Israel, March 6, 2006. 18 pp. URL `http://www.pinkas.net/PAPERS/gpr06.pdf`.

Granger:2005:HSN

[GPS05] R. Granger, D. Page, and M. Stam. Hardware and software normal basis arithmetic for pairing-based cryptography in characteristic three. *IEEE Transactions on Computers*, 54(7):852–860, July 2005. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1432668`.

Granger:2006:SCA

[GPS06] R. Granger, D. Page, and M. Stam. On small characteristic algebraic tori in pairing-based cryptography. *LMS Journal of Computation and Mathematics*, 9:64–85, 2006. CODEN ???? ISSN 1461-1570.

Gentry:2008:THL

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In ACM [ACM08], pages 197–206. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Geng:2008:DSA

[GPX08] Xiutang Geng, Linqiang Pan, and Jin Xu. A DNA sticker algorithm for bit-substitution in a block cipher. *Journal of Parallel and Distributed Computing*, 68(9):1201–1206, September 2008. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Galbraith:2004:EDD

[GR04] Steven D. Galbraith and Victor Rotger. Easy decision Diffie–Hellman groups. *LMS Journal of Computation and Mathematics*, 7: 201–??, 2004. CODEN ???? ISSN 1461-1570.

Grasser:1998:FC

[Gra98] R. Scott Grasser. *FIND-someone.com*. Butterworth-Heinemann, Boston, MA, USA, 1998. ISBN 0-7506-7020-7. xvii + 137 pp. LCCN HV6762.U5 G73 1998. US$39.95.

Graff:2001:CCW

[Gra01] Jon Graff. *Cryptography and e-commerce: a Wiley tech brief*. Wiley tech brief series. John Wiley and Sons, Inc., New York, NY, USA, 2001. ISBN 0-471-40574-4 (paperback). xviii + 222 pp. LCCN QA76.9.A25 G68 2001.

Granboulan:2002:FDC

[Gra02a] Louis Granboulan. Flaws in differential cryptanalysis of Skipjack. *Lecture Notes in Computer Science*, 2355:328–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550328.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550328.pdf.

Granboulan:2002:SSR

[Gra02b] Louis Granboulan. Short signatures in the random oracle model. *Lecture Notes in Computer Science*, 2501:364–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010364.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010364.pdf.

Grigg:2001:FCL

[Gri01] Ian Grigg. Financial cryptography in 7 layers. *Lecture Notes in Computer Science*, 1962:332–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620332.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620332.pdf.

Grossschadl:2001:HSR

[Gro01] Johann Großschädl. High-speed RSA hardware based on Barret's modular reduction method. *Lecture Notes in Computer Science*, 1965:191–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650191.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650191.pdf.

Grossschadl:2003:ASL

[Gro03] Johann Großschädl. Architectural support for long integer modulo arithmetic on RISC-based Smart Cards. *The International Journal of High Performance Computing Applications*, 17(2):135–146, Summer 2003. CODEN IHPCFL. ISSN 1094-3420 (print), 1741-2846 (electronic).

Groth:2005:CS

[Gro05] Jens Groth. Cryptography in subgroups of $\mathbf{Z}*_n$. In

Kilian [Kil05], pages 50–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Gisin:2002:QC

[GRTZ02] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, January 2002. CODEN RMPHAT. ISSN 0034-6861 (print), 1538-4527 (electronic), 1539-0756. URL http://link.aps.org/doi/10.1103/RevModPhys.74.145; http://rmp.aps.org/abstract/RMP/v74/i1/p145_1.

Gentry:2006:EES

[GRW06] Craig Gentry, Zulfikar Ramzan, and David P. Woodruff. Explicit exclusive set systems with applications to broadcast encryption. In IEEE [IEE06], pages 27–38. ISBN 0-7695-2720-5, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S974 2006. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4031329. IEEE Computer Society Order Number P2720.

Geppert:2000:T

[GS00] L. Geppert and W. Sweet. Technology 2000. *IEEE Spectrum*, 37(1):26–31, January 2000. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

GonzalezVasco:2001:CPK

[GS01] María Isabel González Vasco and Rainer Steinwandt. Clouds over a public key cryptosystem based on Lyndon words. *Information Processing Letters*, 80 (5):239–242, 2001. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Garfinkel:2002:WSP

[GS02a] Simson Garfinkel and Gene Spafford. *Web Security, Privacy & Commerce*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, second edition, 2002. ISBN 0-596-00045-6. xxviii + 756 pp. LCCN TK5105.59 .G37 2002 Stacks. US$44.95. URL http://safari.oreilly.com/0596000456; http://www.oreilly.com/catalog/websec2.

Gentry:2002:HIB

[GS02b] Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. *Lecture Notes in Computer Science*, 2501:548–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010548.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010548.pdf.

Gentry:2002:CRN

[GS02c] Craig Gentry and Mike Szydlo. Cryptanalysis of the revised NTRU signature scheme. *Lecture Notes in Computer Science*, 2332:299–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320299.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320299.pdf.

Geiselmann:2003:HSS

[GS03] Willi Geiselmann and Rainer Steinwandt. Hardware to solve sparse systems of linear equations over GF(2). In Walter et al. [WKP03], pages 51–61. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Geiselmann:2007:SPH

[GS07a] Willi Geiselmann and Rainer Steinwandt. Special-purpose hardware in cryptanalysis: The case of 1,024-bit RSA. *IEEE Security & Privacy*, 5(1):63–66, January/February 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Goodell:2007:TOR

[GS07b] Geoffrey Goodell and Paul Syverson. Technical opinion: The right place at the right time. *Communications of the Association for Computing Machinery*, 50(5):113–117, May 2007. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Grassl:2009:CAS

[GS09] Markus Grassl and Rainer Steinwandt. Cryptanalysis of an authentication scheme using truncated polynomials. *Information Process-*

ing Letters, 109(15):861–863, July 16, 2009. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Guida:2004:DUP

[GSB+04] Richard Guida, Robert Stahl, Thomas Bunt, Gary Secrest, and Joseph Moorcones. Deploying and using public key technology: Lessons learned in real life. *IEEE Security & Privacy*, 2(4):67–71, July/August 2004. CODEN ????. ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://csdl.computer.org/dl/mags/sp/2004/04/j4067.htm; http://csdl.computer.org/dl/mags/sp/2004/04/j4067.pdf.

Geetha:2009:BIS

[GSK09] S. Geetha, Siva S. Sivatha Sindhu, and N. Kamaraj. Blind image steganalysis based on content independent statistical measures maximizing the specificity and sensitivity of the system. *Computers & Security*, 28(7):683–697, October 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404809000285.

Garfinkel:2003:PUI

[GSS03] Simson Garfinkel, Gene Spafford, and Alan Schwartz. *Practical Unix & Internet Security*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, third edition, 2003. ISBN 0-596-00323-4. xxix + 954 pp. LCCN QA76.76.O63 G38 2003. US$54.95. URL http://www.oreilly.com/catalog/puis3.

Gaubatz:2008:SCD

[GSS08] G. Gaubatz, E. Savas, and B. Sunar. Sequential circuit design for embedded cryptographic applications resilient to adversarial faults. *IEEE Transactions on Computers*, 57(1):126–138, January 2008. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4358236.

Goodrich:2004:ETB

[GST04] Michael T. Goodrich, Jonathan Z. Sun, and Roberto Tamassia. Efficient tree-based revocation in groups of low-state devices. In Franklin [Fra04], pages 511–?? CODEN LNCSD9.

ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Giles:2002:ADW

[GSVC02] James Giles, Reiner Sailer, Dinesh Verma, and Suresh Chari. Authentication for distributed Web caches. *Lecture Notes in Computer Science*, 2502:126–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2502/25020126.htm; http://link.springer.de/link/service/series/0558/papers/2502/25020126.pdf.

Garay:2000:LLB

[GSW00] Juan A. Garay, Jessica Staddon, and Avishai Wool. Long-lived broadcast encryption. In Bellare [Bel00], pages 333–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800333.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800333.pdf.

Gennaro:2000:LBE

[GT00] R. Gennaro and L. Trevisan. Lower bounds on the efficiency of generic cryptographic constructions. In IEEE [IEE00a], pages 305–313. CODEN ASFPDV. ISBN 0-7695-0850-2, 0-7695-0851-0 (case), 0-7695-0852-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 2000. IEEE Computer Society order number PR00850.

Guttman:2002:ATS

[GT02] Joshua D. Guttman and F. Javier Thayer. Authentication tests and the structure of bundles. *Theoretical Computer Science*, 283(2):333–380, June 2002. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Goodrich:2002:EDD

[GTH02] Michael T. Goodrich, Roberto Tamassia, and Jasminka Hasić. An efficient dynamic and distributed cryptographic accumulator. *Lecture Notes in Computer Science*, 2433:372–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/

0558/bibs/2433/24330372.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330372.pdf.

Goodrich:2003:ADS

[GTTC03] Michael T. Goodrich, Roberto Tamassia, Nikos Triandopoulos, and Robert Cohen. Authenticated data structures for graph and geometric searching. In Joye [Joy03b], pages 295–313. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Goodrich:2008:NFI

[GTY08] Michael T. Goodrich, Roberto Tamassia, and Danfeng (Daphne) Yao. Notarized federated ID management and authentication. *Journal of Computer Security*, 16(4):399–418, ???? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guttman:2004:FAP

[GTZ04] Joshua D. Guttman, F. Javier Thayer, and Lenore D. Zuck. The faithfulness of abstract protocol analysis: Message authentication. *Journal of Computer Security*, 12(6):865–891, ???? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guar:2005:PPL

[Gua05] Nalneesh Guar. Paranoid penguin: Limitations of shc, a shell encryption utility. *Linux Journal*, 2005 (138):11, October 2005. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Guette:2009:ATK

[Gue09] Gilles Guette. Automating trusted key rollover in DNSSEC. *Journal of Computer Security*, 17(6):839–854, ???? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guizzo:2006:BIC

[Gui06] Erico Guizzo. Britain's identity crisis [biometric id cards]. *IEEE Spectrum*, 43(1):42–43, January 2006. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Gumz:2004:BRH

[Gum04] Joy Gumz. Book review: *Hacking Exposed: Network Security Secrets and Solutions*, 4th ed., by Stuart McClure, Joel Scambray, and

George Kurtz, McGraw-Hill, 2003, $49.99, ISBN 0-07-222742-7. *ACM Queue: Tomorrow's Computing Today*, 1(10):88, February 2004. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Guillou:2001:CAP

[GUQ01] L. C. Guillou, M. Ugon, and J-J. Quisquater. Cryptographic authentication protocols for smart cards. *Computer Networks (Amsterdam, Netherlands: 1999)*, 36(4):437–451, July 16, 2001. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.elsevier.nl/gej-ng/10/15/22/61/28/30/abstract.html`; `http://www.elsevier.nl/gej-ng/10/15/22/61/28/30/article.pdf`.

Gutmann:2000:OSC

[Gut00] Peter Gutmann. An open-source cryptographic coprocessor. In USENIX [USE00d], page ?? ISBN 1-880446-18-9. LCCN ???? URL `http://www.usenix.org/publications/library/proceedings/sec2000/gutmann.html`.

Gutmann:2002:CFP

[Gut02a] Peter Gutmann. Cover feature: PKI: It's not dead, just resting. *Computer*, 35(8):41–49, August 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://csdl.computer.org/dl/mags/co/2002/08/r8041.htm`; `http://csdl.computer.org/dl/mags/co/2002/08/r8041.pdf`; `http://www.computer.org/computer/co2002/r8041abs.htm`.

Gutmann:2002:DVC

[Gut02b] Peter Gutmann. *The Design and Verification of a Cryptographic Security Architecture*. PhD thesis, Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand, 2002. URL `http://www.cryptoengines.com/~peter/06_random.pdf`; `http://www.cs.auckland.ac.nz/~pgut001/`; `http://www.cs.auckland.ac.nz/~pgut001/pubs/thesis.html`. Published in book form [Gut04a].

Gutmann:2004:CSA

[Gut04a] Peter Gutmann. *Cryptographic Security Architecture: Design and Verification*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. ISBN 0-387-95387-6. xviii + 320 pp. LCCN QA76.9.A25 G88 2002.

Gutmann:2004:SPK

[Gut04b] Peter Gutmann. Simplifying public key management. *Computer*, 37(2):101–??, February 2004. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/comp/mags/co/2004/02/r2101abs.htm; http://csdl.computer.org/dl/mags/co/2004/02/r2101.htm; http://csdl.computer.org/dl/mags/co/2004/02/r2101.pdf.

Guttman:2004:ATD

[Gut04c] Joshua D. Guttman. Authentication tests and disjoint encryption: A design method for security protocols. *Journal of Computer Security*, 12(3–4):409–433, ???? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gutmann:20xx:ESR

[Gutxx] Peter Gutmann. Encryption and security-related resources. World-Wide Web site., 20xx. URL http://www.cs.auckland.ac.nz/~pgut001/links.html.

Granger:2005:DLP

[GV05] R. Granger and F. Vercauteren. On the discrete logarithm problem on algebraic tori. In Shoup [Sho05a], pages 66–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Garera:2009:CTG

[GV09] Sujata Garera and Jorge Vasconcelos. Challenges in teaching a graduate course in applied cryptography. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 41(2):103–107, June 2009. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Gassend:2008:CPR

[GVC+08] Blaise Gassend, Marten Van Dijk, Dwaine Clarke, Emina Torlak, Srinivas Devadas, and Pim Tuyls. Controlled physical random functions and applications. *ACM Transactions on Information and System Security*, 10 (4):3:1–3:??, January 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gisin:2000:LCQ

[GW00] Nicolas Gisin and Stefan Wolf. Linking classical and quantum key agreement: Is there "Bound Information"? In Bellare [Bel00], pages 482–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800482.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800482.pdf.

Guoxiang:2001:IFB

[GW01] Song Guoxiang and Wang Weiwei. Image-feature based second generation watermarking in wavelet domain. *Lecture Notes in Computer Science*, 2251: 16–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2251/22510016.htm; http://link.springer-ny.com/link/service/series/0558/papers/2251/22510016.pdf.

Gebotys:2008:EAW

[GW08] Catherine H. Gebotys and Brian A. White. EM analysis of a wireless Java-based PDA. *ACM Transactions on Embedded Computing Systems*, 7(4):44:1–44:??, July 2008. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Goldberg:2008:PQM

[GXT+08] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford. Path-quality monitoring in the presence of adversaries. *ACM SIGMETRICS Performance Evaluation Review*, 36(1):193–204, June 2008. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Heys:2000:SAC

[HA00] Howard Heys and Carlisle Adams, editors. *Selected areas in cryptography: 6th annual international workshop, SAC'99, Kingston, Ontario, Canada, August 9–10, 1999: proceedings*, volume 1758 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-67185-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1758. Contents: A universal encryption standard / Helena Handschuh and Serge Vaudenay — Yarrow-160: notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator / John Kelsey, Bruce Schneier, and Niels Ferguson — Elliptic curve pseudorandom sequence generators / Guang Gong, Thomas A. Berson, and Douglas R. Stinson — Adaptive-attack norm for decorrelation and super-pseudorandomness / Serge Vaudenay — Guesswork and variation distance as measures of cipher security / John O. Pliam — Modeling linear characteristics of substitution-permutation networks / Liam Keliher, Henk Meijer, and Stafford Tavares — Strong linear dependence and unbiased distribution of non-propagative vectors / Yuliang Zheng and Xian-Mo Zhang — Security of E2 against truncated differential cryptanalysis / Shiho Moriai ... [et al..] — Key-schedule cryptanalysis of DEAL / John Kelsey and Bruce Schneier — Efficient evaluation of security against generalized interpolation attack / Kazumaro Aoki — Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders / Detlef Huhnlein — Improving and extending the Lim/Lee exponentiation algorithm / Biljana Cubaleska, Andreas Rieke, and Thomas Hermann — Software optimization of decorrelation module / Fabrice Noilhan — Pseudonym systems / Anna Lysyanskaya ... [et al.] — Unconditionally secure proactive secret sharing scheme with combinatorial structures / Douglas R. Stinson and R. Wei — Protecting a mobile agent's route against collusions / Dirk Westhoff ... [et al.] — Photuris: design criteria / William Allen Simpson.

Haddad:2000:AUA

[Had00] Ibrahim F. Haddad. Apache user authentication. *Linux Journal*, 78:??, October 2000. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Hancock:2000:EWP

[Han00] Bill Hancock. Not everyone wants PKI — NSF opts for digital signature alternative. *Computers & Security*, 19(4):301–302, April 1, 2000. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404800040098`.

Harvey:2000:EMA

[Har00] Ian Harvey. The effects of multiple algorithms in the Advanced Encryption Standard. In NIST [NIS00], pages 269–278. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http:`

//csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Hare:2001:RUPa

[Har01a] Chris Hare. Revisiting UNIX password controls – part 1. *Sys Admin: The Journal for UNIX Systems Administrators*, 10(10):30, 32–34, October 2001. CODEN SYADE7. ISSN 1061-2688. URL http://www.samag.com/.

Hare:2001:RUPb

[Har01b] Chris Hare. Revisiting UNIX password controls – part 2. *Sys Admin: The Journal for UNIX Systems Administrators*, 10(11):35–38, November 2001. CODEN SYADE7. ISSN 1061-2688.

Harrington:2005:NSP

[Har05a] Jan L. Harrington. *Network security: a practical approach*. Elsevier, Amsterdam, The Netherlands, 2005. ISBN 0-12-311633-3. xv + 365 pp. LCCN TK5105.59 .H357 2005.

Harris:2005:GHE

[Har05b] Shon Harris, editor. *Gray hat hacking: the ethical hacker's handbook*. All-in-one. Osborne/McGraw-Hill, Berkeley, CA, USA, 2005. ISBN 0-07-225709-1 (paperback). xx + 434 pp. LCCN QA76.9.A25 G743 2005.

Hars:2006:MIA

[Har06] Laszlo Hars. Modular inverse algorithms without multiplications for cryptographic applications. *EURASIP Journal on Embedded Systems*, 2006:1–13, 2006. CODEN ???? ISSN 1687-3955 (print), 1687-3963 (electronic). URL http://downloads.hindawi.com/journals/es/2006/032192.pdf. Article ID 32192.

Harman:2007:PDS

[Har07a] G. (Glyn) Harman. *Prime-detecting sieves*. London Mathematical Society monographs. Princeton University Press, Princeton, NJ, USA, 2007. ISBN 0-691-12437-X. ???? pp. LCCN QA246 .H375 2007. URL http://www.loc.gov/catdir/enhancements/fy0731/2007061051-d.html; http://www.loc.gov/catdir/enhancements/fy0731/2007061051-t.html; http://www.loc.gov/catdir/enhancements/fy0734/2007061051-b.html.

Hars:2007:DIH

[Har07b] Laszlo Hars. Discryption: Internal hard-disk encryption for secure storage. *Computer*, 40(6):103–105, June 2007. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Hasan:2000:LTB

[Has00] M. Anwarul Hasan. Look-up table-based large finite field multiplication in memory constrained cryptosystems. *IEEE Transactions on Computers*, 49(7):749–758, 2000. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Hasan:2001:ECM

[Has01a] M. A. Hasan. Efficient computation of multiplicative inverses for cryptographic applications. In Burgess and Ciminiera [BC01], pages 66–72. ISBN 0-7695-1150-3; 0-7695-1152-X. ISSN 1063-6889. LCCN QA76.9.C62 S95 2001. US$145. URL http://www.acsel-lab.com/arithmetic/arith15/papers/ARITH15_Hasan.pdf. IEEE order no. PR01150.

Hasan:2001:PAA

[Has01b] M. A. Hasan. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems. *IEEE Transactions on Computers*, 50(10):1071–1083, 2001. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Hassler:2002:JCP

[Has02] Vesna Hassler. *Java card for e-payment applications*. Artech House computer security series. Artech House Inc., Norwood, MA, USA, 2002. ISBN 1-58053-291-8. xvii + 362 pp. LCCN QA76.73.J38 J3638 2002.

Haufler:2003:CVH

[Hau03] Hervie Haufler. *Codebreakers' victory: how the Allied cryptographers won World War II*. New American Library, New York, NY, USA, 2003. ISBN 0-451-20979-6. 344 pp. LCCN D810.C88 H38 2003.

Haufler:2006:SWN

[Hau06] Hervie Haufler. *The spies who never were: the true story of the Nazi spies who were actually Allied double agents*. NAL Caliber, New York, NY, USA, 2006. ISBN 0-451-21751-9 (paperback). ???? pp. LCCN D810.S7 H37 2006. URL http://www.loc.gov/catdir/toc/ecip0517/2005022622.html.

Hayat:2004:CSE

[HAuR04] Khawaja Amer Hayat, Umar Waqar Anis, and

S. Tauseef ur Rehman. Cryptanalysis of some encryption/cipher schemes using related key attack. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 36(4):85–87, December 2004. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). NOTE FROM ACM: It has been determined that the authors of this article plagiarized the contents from a previously published paper. Therefore ACM has shut off access to this paper.

Hayashi:2006:QIT

[Hay06] Masahito Hayashi. *Quantum Information Theory: An Introduction*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-540-30265-4. LCCN ???? URL `http://www.springer.com/dal/home?SGWID=1-102-22-100724694-0`.

Hoglund:2006:RSW

[HB06] Greg Hoglund and James Butler. *Rootkits: subverting the Windows kernel*. Addison-Wesley, Reading, MA, USA, 2006. ISBN 0-321-29431-9 (paperback). xxiii + 324 pp. LCCN QA76.9.A25 H637 2006. URL `http://www.loc.gov/catdir/toc/ecip0512/2005013061.html`.

Huffmire:2008:DSS

[HBC+08] Ted Huffmire, Brett Brotherton, Nick Callegari, Jonathan Valamehr, Jeff White, Ryan Kastner, and Tim Sherwood. Designing secure systems on reconfigurable hardware. *ACM Transactions on Design Automation of Electronic Systems*, 13(3):44:1–44:??, July 2008. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Hartel:2001:TMS

[HBdJL01] Pieter H. Hartel, Michael J. Butler, Eduard de Jong, and Mark Longley. Transacted memory for smart cards. *Lecture Notes in Computer Science*, 2021: 478–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2021/20210478.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2021/20210478.pdf`.

Holcomb:2009:PSS

[HBF09] D. E. Holcomb, W. P. Burleson, and K. Fu. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Transactions on Computers*, 58(9):1198–1210, September 2009. CO-

DEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4674345.

Humphries:2002:IC

[HC02] Jeffrey W. Humphries and Martin C. Carlisle. Introduction to Cryptography. *ACM Journal on Educational Resources in Computing (JERIC)*, 2(3): 2, September 2002. CODEN ???? ISSN 1531-4278.

Huang:2004:NDE

[HC04a] Hui-Feng Huang and Chin-Chen Chang. A new design of efficient partially blind signature scheme. *The Journal of Systems and Software*, 73(3):397–403, November/ December 2004. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Hwang:2004:NMP

[HC04b] Shin-Jia Hwang and Chiu-Chin Chen. New multi-proxy multi-signature schemes. *Applied Mathematics and Computation*, 147(1):57–67, January 5, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Huang:2008:NCK

[HC08] Hui-Feng Huang and Chin-Chen Chang. A novel cryptographic key assignment scheme with ID-based access control in a hierachy. *Fundamenta Informaticae*, 84(3–4):353–361, September 2008. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Hernandez-Castro:2006:SGG

[HCBLETRG06] Julio C. Hernandez-Castro, Ignacio Blasco-Lopez, Juan M. Estevez-Tapiador, and Arturo Ribagorda-Garnacho. Steganography in games: a general methodology and its application to the game of go. *Computers & Security*, 25(1):64–71, February 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404805002002.

Han:2008:PBPa

[HCD08a] Song Han, Elizabeth Chang, and Tharam Dillon. Pairing-based public-key encryption schemes with backward-and-forward security. *International Journal of Computer Systems Science and Engineering*, 23(1):??, January 2008. CODEN CSSEEI. ISSN 0267-6192.

Han:2008:PBPb

[HCD08b] Song Han, Elizabeth Chang, and Tharam Dillon. Pairing-based public-key encryption schemes with backward-and-forward security. *International Journal of Computer Systems Science and Engineering*, 23(4):??, July 2008. CODEN CSSEEI. ISSN 0267-6192.

Henderson:2002:MTS

[HCDO02] Marie Henderson, Robert Coulter, Ed Dawson, and Eiji Okamoto. Modelling trust structures for public key infrastructures. *Lecture Notes in Computer Science*, 2384:56–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840056.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840056.pdf.

Halevi:2002:SSE

[HCJ02] Shai Halevi, Don Coppersmith, and Charanjit Jutla. Scream: a software-efficient stream cipher. *Lecture Notes in Computer Science*, 2365:195–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650195.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650195.pdf.

Han:2009:ICS

[HCK09] Dong-Guk Han, Dooho Choi, and Howon Kim. Improved computation of square roots in specific finite fields. *IEEE Transactions on Computers*, 58(2):188–196, February 2009. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4663058.

He:2002:WSM

[He02] Wei-Hua He. Weaknesses in some multisignature schemes for specified group of verifiers. *Information Processing Letters*, 83(2):95–99, July 31, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Heger:2009:CTQ

[Heg09] M. Heger. Cryptographers take on quantum computers — [update]. *IEEE Spectrum*, 46(1):14, January 2009. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Heijl:2001:DXS

[Hei01] Danny Heijl. The Delphi XML SAX2 component and MSXML 3.0. *Dr. Dobb's Journal of Software Tools*, 26(9):42, 46, 48, 50, 52, 54, September 2001. CODEN DDJOEB. ISSN 1044-

789X. URL http://www.ddj.com/ftp/2001/2001_09/xmlsax2.txt; http://www.ddj.com/ftp/2001/2001_09/xmlsax2.zip. See correction [TEM+01].

Heiser:2003:BCB

[Hei03] Jay G. Heiser. Beyond cryptography: Bruce Schneier's beyond fear: thinking sensibly about security in an uncertain world. *Computers & Security*, 22(8):673–674, December 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803000051.

Heikkila:2007:ESC

[Hei07] Faith M. Heikkila. Encryption: Security considerations for portable media devices. *IEEE Security & Privacy*, 5(4):22–27, July/August 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Hendry:2001:SCS

[Hen01] Mike Hendry. *Smart card security and applications*. The Artech House telecommunications library. Artech House Inc., Norwood, MA, USA, second edition, 2001. ISBN 1-58053-156-3. xviii + 305 pp. LCCN TK7895.S62 H46 2001.

Henderson:2006:CBG

[Hen06a] Roger William Henderson. *Cryptanalysis of braid group cryptosystem and related combinatorial structures*. Thesis (Ph.D.), University of London, London, UK, 2006. ???? pp.

Henry:2006:TFA

[Hen06b] Paul A. Henry. Two-factor authentication — a look behind the headlines. *Network Security*, 2006(4):18–19, April 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485806703609.

Herzberg:2002:SX

[Her02] Amir Herzberg. Securing XML. *Dr. Dobb's Journal of Software Tools*, 27 (3):56, 59–62, March 2002. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ftp/2002/2002_03/secxml.txt.

Herranz:2006:DIB

[Her06] Javier Herranz. Deterministic identity-based signatures for partial aggregation. *The Computer Journal*, 49(3): 322–330, May 2006. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/49/3/322; http://comjnl.

oxfordjournals.org/cgi/content/full/49/3/322; http://comjnl.oxfordjournals.org/cgi/reprint/49/3/322.

Herranz:2007:IBR

[Her07] Javier Herranz. Identity-based ring signatures from RSA. *Theoretical Computer Science*, 389(1–2):100–117, December 10, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Heron:2009:AES

[Her09a] Simon Heron. Advanced Encryption Standard (AES). *Network Security*, 2009(12): 8–12, December 2009. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485810700064.

Herzberg:2009:DBE

[Her09b] Amir Herzberg. DNS-based email sender authentication mechanisms: a critical review. *Computers & Security*, 28(8):731–742, November 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404809000492.

Hess:2004:SVE

[Hes04a] F. Hess. On the security of the verifiably-encrypted signature scheme of Boneh, Gentry, Lynn and Shacham. *Information Processing Letters*, 89(3):111–114, February 14, 2004. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hess:2004:GAR

[Hes04b] Florian Hess. The GHS attack revisited. *LMS Journal of Computation and Mathematics*, 7:167–??, 2004. CODEN ???? ISSN 1461-1570.

Heys:2003:ASC

[Hey03] H. M. Heys. Analysis of the statistical cipher feedback mode of block ciphers. *IEEE Transactions on Computers*, 52(1):77–92, January 2003. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1159755.

Hassler:2000:OFA

[HF00] Vesna Hassler and Oliver Fodor. OpenCard Framework application development. *Dr. Dobb's Journal of Software Tools*, 25(2):70, 72, 74–76, February 2000. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ftp/2000/2000_02/ocfjava.txt; http://www.ddj.com/ftp/2000/2000_02/ocfjava.zip.

Horvitz:2003:WKA

[HG03] Omer Horvitz and Virgil Gligor. Weak key authenticity and the computational completeness of formal encryption. In Boneh [Bon03], pages 530–547. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Horan:2005:NRN

[HG05a] D. M. Horan and R. A. Guinee. A novel random number generator based on pseudonoise sequences. *IEE Conference Publications*, 2005 (CP511):431–436, 2005. CODEN ???? ISSN ???? URL http://link.aip.org/link/abstract/IEECPS/v2005/iCP511/p431/s1.

Howgrave-Graham:2005:PKC

[HG05b] Nick Howgrave-Graham. Public-key cryptography and proofs of security. In Garrett and Lieman [GL05], pages 73–89. ISBN 0-8218-3365-0. LCCN QA76.9.A25 P82 2005. URL http://www.loc.gov/catdir/toc/fy0612/2005048178.html.

Howgrave-Graham:2007:HLR

[HG07] Nick Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In Menezes [Men07], pages 150–169. ISBN 3-540-74142-9 (paperback). LCCN QA76.9.A25 C79 2007. URL http://portal.acm.org/citation.cfm?id=1777777.1777791.

Hasenplaugh:2007:FMR

[HGG07] William Hasenplaugh, Gunnar Gaubatz, and Vinodh Gopal. Fast modular reduction. In Kornerup and Muller [KM07], pages 225–229. ISBN 0-7695-2854-6. ISSN 1063-6889. LCCN ???? URL http://www.lirmm.fr/arith18/.

Howgrave-Graham:2003:IDF

[HGNP+03] Nick Howgrave-Graham, Phong Q. Nguyen, David Pointcheval, John Proos, Joseph H. Silverman, Ari Singer, and William Whyte. The impact of decryption failures on the security of NTRU encryption. In Boneh [Bon03], pages 226–246. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25

C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Howgrave-Graham:2003:HNP

[HGNS03] Nick A. Howgrave-Graham, Phong Q. Nguyen, and Igor E. Shparlinski. Hidden number problem with hidden multipliers, timed-release crypto, and noisy exponentiation. *Mathematics of Computation*, 72(243):1473–1485, July 2003. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journal-getitem?pii=S0025-5718-03-01495-9; http://www.ams.org/mcom/2003-72-243/S0025-5718-03-01495-9/S0025-5718-03-01495-9.dvi; http://www.ams.org/mcom/2003-72-243/S0025-5718-03-01495-9/S0025-5718-03-01495-9.pdf; http://www.ams.org/mcom/2003-72-243/S0025-5718-03-01495-9/S0025-5718-03-01495-9.ps; http://www.ams.org/mcom/2003-72-243/S0025-5718-03-01495-9/S0025-5718-03-01495-9.tex.

Hendricks:2007:LOB

[HGR07] James Hendricks, Gregory R. Ganger, and Michael K. Reiter. Low-overhead Byzantine fault-tolerant storage. *Operating Systems Review*, 41(6):73–86, December 2007. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Handschuh:2004:SAC

[HH04] Helena Handschuh and M. Anwar Hasan, editors. *Selected Areas in Cryptography: 11th international workshop, SAC 2004, Waterloo, Canada, August 9–10, 2004: Revised selected papers*, volume 3357 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-24327-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 S22 2004. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3357; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b105103.

Handschuh:2005:SAC

[HH05] Helena Handschuh and M. Anwar Hasan, editors. *Selected areas in cryptog-*

raphy: 11th international workshop, SAC 2004, Waterloo, Canada, August 9–10, 2004: Revised selected papers, volume 3357 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-24327-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 S22 2004. URL `http://springerlink.metapress.com/openurl.asp?genre=issue&issn=0302-9743&volume=3357`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3357`.

Hung:2009:FBA

[HH09] Kuo Lung Hung and Shin-Wei He. Feature based affine invariant watermarking robust to geometric distortions. *Fundamenta Informaticae*, 92(1–2):131–143, January 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Hwang:2005:TSP

[HHC05] Min-Shiang Hwang, Kuo-Feng Hwang, and Chin-Chen Chang. A time-stamping protocol for digital watermarking. *Applied Mathematics and Computation*, 169(2):1276–1284, October 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hoffstein:2006:NNE

[HHG06] J. Hoffstein and N. Howgrave-Graham. NTRUEncrypt and NTRUSign: efficient public-key algorithms for a post-quantum world. In *PQCrypto 2006: International Workshop on Post-Quantum Cryptography*, pages 141–158. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN ???? LCCN ????

Hoffstein:2003:NDS

[HHGP+03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. NTRUSIGN: Digital signatures using the NTRU lattice. In Joye [Joy03b], pages 122–140. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612`.

Hess:2004:CTT

[HHJS04] Adam Hess, Jason Holt, Jared Jacobson, and Kent E. Seamons. Content-triggered trust negotiation. *ACM Transactions on Information and System Security*, 7 (3):428–456, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Hong:2004:DCT

[HHK+04] Seokhie Hong, Deukjo Hong, Youngdai Ko, Donghoon Chang, Wonil Lee, and Sangjin Lee. Differential cryptanalysis of TEA and XTEA. *Lecture Notes in Computer Science*, 2971: 402–417, 2004. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/n4exvw35x7g8t6pb/`.

Hankerson:2000:CTC

[HHL+00] Darrel R. Hankerson, Gary Hoffman, D. A. Leonard, Charles C. Lindner, K. T. Phelps, C. A. Rodger, and J. R. Wall. *Coding theory and cryptography: the essentials*, volume 234 of *Monographs and textbooks in pure and applied mathematics*. Marcel Dekker, Inc., New York, NY, USA, second edition, 2000. ISBN 0-8247-0465-7. x + 350 pp. LCCN QA268 .C675 2000. URL `http://lccn.loc.gov/00060106`.

Hankerson:2001:SIE

[HHM01] Darrel Hankerson, Julio López Hernandez, and Alfred Menezes. Software implementation of elliptic curve cryptography over binary fields. *Lecture Notes in Computer Science*, 1965: 1–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650001.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1965/19650001.pdf`.

Hamann:2001:SBA

[HHSS01] E.-M. Hamann, H. Henn, T. Schäck, and F. Seliger. Securing e-business applications using smart cards. *IBM Systems Journal*, 40 (3):635–647, ???? 2001. CODEN IBMSA7. ISSN 0018-8670. URL `http://www.research.ibm.com/journal/sj/403/hamann.html`; `http://www.research.ibm.com/journal/sj/403/hamann.pdf`.

Han:2007:FIE

[HHYW07] Fengling Han, Jiankun Hu, Xinghuo Yu, and Yi Wang. Fingerprint images encryption via multi-scroll chaotic attractors. *Applied Mathematics and Computation*, 185(2):931–939, February 15, 2007. CODEN AMHCBQ. ISSN 0096-3003

(print), 1873-5649 (electronic).

Hernandez:2004:FED

[HI04] Julio C. Hernandez and Pedro Isasi. Finding efficient distinguishers for cryptographic mappings, with an application to the block cipher TEA. *Computational Intelligence*, 20(3):517–525, August 2004. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Higgins:2008:NSC

[Hig08] Peter M. Higgins. *Number story: from counting to cryptography*. Copernicus, New York, NY, USA, 2008. ISBN 1-84800-000-6 (hardcover), 1-84800-001-4 (ebook). 323 pp. LCCN QA241 .H48 2008. URL http://www.loc.gov/catdir/toc/fy0804/2007936363.html.

Hill:2000:KII

[Hil00] Paul B. Hill. Kerberos interoperability issues. In USENIX [USE00a], page ?? ISBN 1-880446-19-7. LCCN ???? URL http://db.usenix.org/publications/library/proceedings/lisa-nt2000/hill.html.

Hilley:2005:CRM

[Hil05] Sarah Hilley. Crypto race for mathematical infinity. *Network Security*, 2005(4): 10–11, April 2005. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485805702233.

Hilley:2006:SSD

[Hil06] Sarah Hilley. Secret Service dismantles web forums. *Network Security*, 2006(4): 20, April 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485806703610.

Hacigumus:2002:ESE

[HILM02] Hakan Hacigümüş, Bala Iyer, Chen Li, and Sharad Mehrotra. Executing SQL over encrypted data in the database-service-provider model. In Franklin et al. [FMA02], pages 216–227. ISBN ???? LCCN ???? ACM order number 475020.

Hirose:2009:SAD

[Hir09] S. Hirose. Security analysis of DRBG using HMAC in NIST SP 800-90. In Chung et al. [CSY09], pages 278–291. CODEN LNCSD9. ISBN 3-642-00305-2 (print), 3-642-00306-0 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/

content/978-3-642-00306-6.

Hinkelmann:2007:CUN

[HJ07] Markus Hinkelmann and Andreas Jakoby. Communications in unknown networks: Preserving the secret of topology. *Theoretical Computer Science*, 384(2–3):184–200, October 1, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Huhnlein:2001:TPN

[HJW01] Detlef Hühnlein, Michael J. Jacobson, Jr., and Damian Weber. Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders (extended abstract). *Lecture Notes in Computer Science*, 2012: 275–287, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120275.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120275.pdf.

Huang:2005:ASE

[HJW05] Qiang Huang, David Jao, and Helen J. Wang. Applications of secure electronic voting to automated privacy-preserving troubleshooting. In Meadows and Syverson [MS05b], pages 68–80. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Harris:2005:IUS

[HKA+05] David Harris, Ram Krishnamurthy, Mark Anders, Sanu Mathew, and Steven Hsu. An improved unified scalable radix-2 Montgomery multiplier. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL http://arith17.polito.it/final/paper-109.pdf.

Kim:2000:RMW

[hKLS00] Tae hoon Kim, Jehee Lee, and Sung Yong Shin. Robust motion watermarking based on multiresolution analysis. *Computer Graphics Forum*, 19(3): ??, August 2000. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic). URL aid=411& http://www.blackwellpublishers.co.uk/asp/journal.asp?ref=0167-7055& iid=3& src=ard& vid=19.

Heuberger:2005:AGE

[HKPR05] Clemens Heuberger, Rajendra Katti, Helmut Prodinger, and Xiaoyu Ruan. The alternating greedy expansion and applications to computing digit expansions from left-to-right in cryptography. *Theoretical Computer Science*, 341(1–3):55–72, September 5, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Handschuh:2001:ASE

[HKR01] Helena Handschuh, Lars R. Knudsen, and Matthew J. Robshaw. Analysis of SHA-1 in encryption mode. In *Topics in cryptology—CT-RSA 2001 (San Francisco, CA)*, volume 2020 of *Lecture Notes in Comput. Sci.*, pages 70–83. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200070.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200070.pdf`.

Hofmeister:2000:COS

[HKS00] Thomas Hofmeister, Matthias Krause, and Hans U. Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Theoretical Computer Science*, 240(2):471–485, June 17, 2000. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.nl/gej-ng/10/41/16/174/23/31/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/174/23/31/article.pdf`.

Hiltgen:2006:SIB

[HKW06] Alain Hiltgen, Thorsten Kramp, and Thomas Weigold. Secure Internet banking authentication. *IEEE Security & Privacy*, 4(2):21–29, March/April 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Horwitz:2002:THI

[HL02] Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-based encryption. *Lecture Notes in Computer Science*, 2332: 466–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320466.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320466.pdf`.

Howard:2003:WSC

[HL03] Michael Howard and David LeBlanc. *Writing secure code*. Microsoft Press, Redmond, WA, USA, second edition, 2003. ISBN 0-7356-1722-8. xxviii + 768 pp. LCCN QA76.9.A25 H698 2003.

Hwang:2004:REL

[HL04] Shin-Jia Hwang and Yun-Hua Lee. Repairing ElGamal-like multi-signature schemes using self-certified public keys. *Applied Mathematics and Computation*, 156(1):73–83, August 25, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hohenberger:2005:HSO

[HL05a] Susan Hohenberger and Anna Lysyanskaya. How to securely outsource cryptographic computations. In Kilian [Kil05], pages 264–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171`.

Hwang:2005:TAU

[HL05b] Kuo-Feng Hwang and I-En Liao. Two attacks on a user friendly remote authentication scheme with Smart Cards. *Operating Systems Review*, 39(2):94–96, April 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Hwang:2005:SHW

[HL05c] Shin-Jia Hwang and Hao-Chih Liao. Security of Hsu–Wu's authenticated encryption scheme with (t, n) shared verification. *Applied Mathematics and Computation*, 167(1):281–285, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hwang:2005:STH

[HL05d] Shin-Jia Hwang and Hao-Chih Liao. Security of Tzeng–Hwang's authenticated encryption scheme based on elliptic curve discrete logarithm problems. *Applied Mathematics and Computation*, 168(1):717–721, September 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Howard:2006:SDL

[HL06] Michael Howard and Steve Lipner. *The security development lifecycle: SDL, a process for developing demonstrably more secure software*. Secure software development series. Microsoft Press, Redmond, WA, USA, 2006. ISBN 0-7356-2214-0. xxii + 320 pp. LCCN QA76.76.D47 H74 2006.

Huang:2007:EPS

[HL07] Chung-Ming Huang and Jian-Wei Li. Efficient and provably secure IP multimedia subsystem authentication for UMTS. *The Computer Journal*, 50(6):739–757, November 2007. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/cgi/content/abstract/50/6/739; http://comjnl.oxfordjournals.org/cgi/content/full/50/6/739; http://comjnl.oxfordjournals.org/cgi/reprint/50/6/739`.

Hu:2007:DWD

[HLC07] Ming-Chiang Hu, Der-Chyuan Lou, and Ming-Chang Chang. Dual-wrapped digital watermarking scheme for image copyright protection. *Computers & Security*, 26(4):319–330, June 2007. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404806002070`.

Hwang:2008:CPK

[HLC08] Y. H. Hwang, J. K. Liu, and S. S. Chow. Certificateless public key encryption secure against malicious KGC attacks in the standard model. *J.UCS: Journal of Universal Computer Science*, 14(3):463–480, ???? 2008. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_14_3/certificateless_public_key_encryption`.

Hwang:2000:CBV

[HLH00] Min-Shiang Hwang, Iuon-Chung Lin, and Kuo-Feng Hwang. Cryptanalysis of the batch verifying multiple RSA digital signatures. *Informatica (Vilnius)*, 11(1):15–18, 2000. ISSN 0868-4952.

Hong:2001:PSA

[HLL+01] Seokhie Hong, Sangjin Lee, Jongin Lim, Jaechul Sung, Donghyeon Cheon, and Inho Cho. Provable security against differential and linear cryptanalysis for the SPN structure. *Lecture Notes in Computer Science*, 1978:273–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780273.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780273.pdf`.

Han:2002:DMA

[HLL+02] Hong Han, Xian Liang Lu, Jun Lu, Chen Bo, and Ren Li Yong. Data mining aided signature discovery in network-based intrusion detection system. *Operating*

Systems Review, 36(4):7–13, October 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Hwang:2003:TRB

[HLL03] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai. Traceability on RSA-based partially signature with low computation. *Applied Mathematics and Computation*, 145(2–3):465–468, December 25, 2003. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hwang:2004:KAS

[HLL04] Min-Shiang Hwang, Li-Hua Li, and Cheng-Chi Lee. A key authentication scheme with non-repudiation. *Operating Systems Review*, 38 (3):75–78, July 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Hwang:2005:GTS

[HLL05] Jung Yeon Hwang, Dong Hoon Lee, and Jongin Lim. Generic transformation for scalable broadcast encryption schemes. In Shoup [Sho05a], pages 276–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Hong:2003:BBP

[HLLL03] Hyun-Soo Hong, Ho-Kyu Lee, Hyang-Sook Lee, and Hee-Jung Lee. The better bound of private key in RSA with unbalanced primes. *Applied Mathematics and Computation*, 139(2–3):351–362, July 15, 2003. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Herzog:2003:PAK

[HLM03] Jonathan Herzog, Moses Liskov, and Silvio Micali. Plaintext awareness via key registration. In Boneh [Bon03], pages 548–564. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Hwang:2001:TSB

[HLT01] Min-Shiang Hwang, Cheng-

Chi Lee, and Yuan-Liang Tang. Two simple batch verifying multiple digital signatures. *Lecture Notes in Computer Science*, 2229: 233–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290233.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290233.pdf.

Huang:2009:OSW

[HLTJ09] Y. L. Huang, P. H. Lu, J. D. Tygar, and A. D. Joseph. OSNP: Secure wireless authentication protocol using one-time key. *Computers & Security*, 28(8):803–815, November 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404809000558.

Hopper:2002:PSS

[HLvA02] Nicholas J. Hopper, John Langford, and Luis von Ahn. Provably secure steganography: (extended abstract). In Yung [Yun02a], pages 77–92. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420077.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420077.pdf.

Hu:2009:TRN

[HLwWZ09] Yue Hu, Xiaofeng Liao, Kwok wo Wong, and Qing Zhou. A true random number generator based on mouse movement and chaotic cryptography. *Chaos, solitons & fractals*, 40(5):2286–2293, 2009. CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic).

Hamdy:2000:SCB

[HM00] Safuat Hamdy and Bodo Möller. Security of cryptosystems based on class groups of imaginary quadratic orders. *Lecture Notes in Computer Science*, 1976: 234–247, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hartel:2001:FSJ

[HM01a] Pieter H. Hartel and Luc Moreau. Formalizing the safety of Java, the Java Virtual Machine, and Java card. *ACM Computing Surveys*, 33(4):517–558, December 2001. CODEN CMSVAN. ISSN 0360-0300

(print), 1557-7341 (electronic).

Hirt:2001:RFU

[HM01b] Martin Hirt and Ueli Maurer. Robustness for free in unconditional multi-party computation. In Kilian [Kil01a], pages 101–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390101.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390101.pdf`.

Harbitter:2002:MAP

[HM02a] Alan Harbitter and Daniel A. Menascé. A methodology for analyzing the performance of authentication protocols. *ACM Transactions on Information and System Security*, 5(4):458–491, November 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Hevia:2002:PSG

[HM02b] Alejandro Hevia and Daniele Micciancio. The provable security of graph-based one-time signatures and extensions to algebraic signature schemes. *Lecture Notes in Computer Science*, 2501: 379–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2501/25010379.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010379.pdf`.

Hitchcock:2002:NEC

[HM02c] Yvonne Hitchcock and Paul Montague. A new elliptic curve scalar multiplication algorithm to resist simple power analysis. *Lecture Notes in Computer Science*, 2384:214–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840214.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840214.pdf`.

Hoglund:2004:ESH

[HM04] Greg Hoglund and Gary McGraw. *Exploiting software: how to break code*. Addison-Wesley, Reading, MA, USA, 2004. ISBN 0-201-78695-8 (paperback). xxxv + 471 pp. LCCN QA76.9.A25 H635 2004. URL `http://www.loc.gov/catdir/toc/ecip0411/2003025556.html`.

Hollar:2005:EWS

[HM05] Rickland Hollar and Richard Murphy. *Enterprise Web services security*. Charles River Media, Hingham, MA, USA, 2005. ISBN 1-58450-413-7 (pbk. with CD-ROM). ???? pp. LCCN TK5105.59 .H66 2005. URL http://www.loc.gov/catdir/toc/ecip0515/2005018419.html.

Holenstein:2004:CCB

[HMS04] Thomas Holenstein, Ueli Maurer, and Johan Sjödin. Complete classification of bilinear hard-core functions. In Franklin [Fra04], pages 73–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Hankerson:2004:GEC

[HMV04] Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. ISBN 0-387-95273-X. xx + 311 pp. LCCN QA76.9.A25 H37 2003. US$59.95.

Huang:2007:MPK

[HMvdLM07] Dijiang Huang, Manish Mehta, Appie van de Liefvoort, and Deep Medhi. Modeling pairwise key establishment for random key predistribution in large-scale sensor networks. *IEEE/ACM Transactions on Networking*, 15(5):1204–1215, October 2007. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Haastad:2004:SAR

[HN04] Johan Håstad and Mats Nåslund. The security of all RSA and discrete log bits. *Journal of the ACM*, 51(2):187–230, March 2004. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Harnik:2006:CNI

[HN06] Danny Harnik and Moni Naor. On the compressibility of NP instances and cryptographic applications. In IEEE [IEE06], pages 719–728. ISBN 0-7695-2720-5, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S974 2006. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4031329. IEEE Computer Society Order Number P2720.

Hiary:2007:SSE

[HN07] Hazem Hiary and Kia Ng. A system for segmenting and extracting paper-based watermark designs. *International Journal on Digital Libraries*, 6(4):351–361, July 2007. CODEN ???? ISSN 1432-1300 (print), 1432-5012 (electronic). URL https://link.springer.com/article/10.1007/s00799-007-0008-7.

Haitner:2009:SHC

[HNO+09] Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, Omer Reingold, and Salil Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM Journal on Computing*, 39(3):1153–1218, ???? 2009. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Hanaoka:2002:HNI

[HNZI02] Goichiro Hanaoka, Tsuyoshi Nishioka, Yuliang Zheng, and Hideki Imai. A hierarchical non-interactive key-sharing scheme with low memory size and high resistance against collusion attacks. *The Computer Journal*, 45(3):293–303, ???? 2002. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_03/450293.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_03/pdf/450293.pdf.

Hoepman:2001:SKA

[Hoe01] Jaap-Henk Hoepman. Secret key authentication with software-only verification. *Lecture Notes in Computer Science*, 1962: 313–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620313.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620313.pdf.

Hofinger:2001:LBE

[Höf01] Siegfried Höfinger. Load balancing for the electronic structure program GREMLIN in a very heterogeneous SSH-connected WAN-cluster of UNIX-type hosts. *Lecture Notes in Computer Science*, 2074: 801–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2074/20740801.htm; http://link.springer-ny.com/link/service/series/

0558/papers/2074/20740801.pdf.

Honary:2001:CCI

[Hon01] Bahram Honary, editor. *Cryptography and coding: 8th IMA international conference, Cirencester, UK, December 17–19, 2001: proceedings*, volume 2260 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-43026-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C76 2001. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2260.htm.

Hook:2005:BCP

[Hoo05] David Hook. *Beginning cryptography and PKI in Java*. John Wiley and Sons, Inc., New York, NY, USA, 2005. ISBN 0-7645-9633-0. xxvi + 448 pp. LCCN QA76.9.A25 H645 2005. URL http://www.loc.gov/catdir/toc/ecip0511/2005011272.html.

Hoskins:2006:SO

[Hos06a] Matthew E. Hoskins. Securing openSSH. *Linux Journal*, 2006(147):??, July 2006. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Hoskins:2006:SSE

[Hos06b] Matthew E. Hoskins. SSHFS: super easy file access over SSH. *Linux Journal*, 2006 (146):??, June 2006. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Horn:2000:APF

[HP00] Günther Horn and Bart Preneel. Authentication and payment in future mobile systems. *Journal of Computer Security*, 8(2–3):183–207, ???? 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Huhnlein:2001:ICB

[HP01] Detlef Hühnlein and Sachar Paulus. On the implementation of cryptosystems based on real quadratic number fields (extended abstract). *Lecture Notes in Computer Science*, 2012: 288–302, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Han:2002:CMV

[HPC02] Daewan Han, Sangwoo Park, and Seongtaek Chee. Cryptanalysis of the modified version of the hash function proposed at PKC'98. *Lecture Notes in Computer Science*, 2365:252–??, 2002. CODEN LNCSD9. ISSN

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650252.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650252.pdf.

Hoffstein:2001:NNL

[HPS01] J. Hoffstein, J. Pipher, and J. H. Silverman. NSS: An NTRU lattice-based signature scheme. In Pfitzmann [Pfi01], pages 211–228. ISBN 3-540-42070-3. LCCN QA76.9.A25 E964 2001; QA76.9.A25 E96 2001. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2045.htm; http://link.springer.de/link/service/series/0558/tocs/t2045.htm.

Hoffstein:2008:IMC

[HPS08] Jeffrey Hoffstein, Jill Catherine Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*, volume 666 of *Undergraduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 0-387-77993-0 (hardcover). xv + 523 pp. LCCN QA268 .H64 2008.

He:2001:SAR

[HQ01] Yeping He and Sihan Qing. Square attack on reduced Camellia cipher. *Lecture Notes in Computer Science*, 2229:238–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290238.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290238.pdf.

Hu:2005:USA

[HQ05] Ruo Hu and Xingsan Qian. Using smart agent-based method to implement dynamic information security policy. In Han et al. [HYZ05b], pages 131–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Hawkes:2001:PCS

[HQR01] Philip Hawkes, Frank Quick, and Gregory G. Rose. A practical cryptanalysis of SSC2. *Lecture Notes in Computer Science*, 2259:25–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590025.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590025.pdf.

Hawkes:2000:EMC

[HR00] Philip Hawkes and Gregory G. Rose. Exploiting multiples of the connection polynomial in word-oriented stream ciphers. *Lecture Notes in Computer Science*, 1976:303–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760303.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760303.pdf.

Hand:2002:MPP

[HR02] Steven Hand and Timothy Roscoe. Mnemosyne: Peer-to-peer steganographic storage. *Lecture Notes in Computer Science*, 2429:130–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2429/24290130.htm; http://link.springer.de/link/service/series/0558/papers/2429/24290130.pdf.

Halevi:2003:TEM

[HR03] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In Boneh [Bon03], pages 482–499. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Hawkes:2004:RVC

[HR04a] Philip Hawkes and Gregory G. Rose. Rewriting variables: The complexity of fast algebraic attacks on stream ciphers. In Franklin [Fra04], pages 390–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Hsiao:2004:FCP

[HR04b] Chun-Yuan Hsiao and Leonid Reyzin. Finding collisions on a public road, or do secure hash functions need secret coins? In Franklin [Fra04], pages 92–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-

3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Holenstein:2005:OWS

[HR05] Thomas Holenstein and Renato Renner. One-way secret-key agreement and applications to circuit polarization and immunization of public-key encryption. In Shoup [Sho05a], pages 478–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Halevi:2006:TCT

[HR06] Shai Halevi and Tal Rabin, editors. *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4–7, 2006. Proceedings*, volume 3876 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-32731-2 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3876.

Haitner:2007:SHC

[HR07] Iftach Haitner and Omer Reingold. Statistically-hiding commitment from any one-way function. In ACM [ACM07], pages 1–10. ISBN 1-59593-631-9. LCCN QA75.5 .A22 2007.

He:2013:GME

[HR13] Q. Y. He and M. D. Reid. Genuine multipartite Einstein–Podolsky–Rosen steering. *Physical Review Letters*, 111(25): 250403, December 2013. CODEN PRLTAO. ISSN 0031-9007 (print), 1079-7114 (electronic), 1092-0145. URL http://link.aps.org/doi/10.1103/PhysRevLett.111.250403; http://www.scientificcomputing.com/news/2014/03/einsteins-entanglement-produces-quantum-encryption; http://www.swinburne.edu.au/engineering/caous/news_and_events/mulitipartite%20EPR%20steering%20paper.htm.

Harn:2009:DDB

[HRL09] Lein Harn, Jian Ren, and

Changlu Lin. Design of DL-based certificateless digital signatures. *The Journal of Systems and Software*, 82(5):789–793, May 2009. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Hromkovic:2003:AHP

[Hro03] Juraj Hromkovič. *Algorithmics for Hard Problems: Introduction to Combinatorial Optimization, Randomization, Approximation, and Heuristics*. Texts in theoretical computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2003. ISBN 3-540-44134-4. xiii + 544 pp. LCCN QA76.58 .H76 2003. URL http://www.loc.gov/catdir/enhancements/fy0817/2002032405-d.html; http://www.loc.gov/catdir/enhancements/fy0817/2002032405-t.html.

Hromkovic:2005:DAR

[Hro05] Juraj Hromkovič. *Design and analysis of randomized algorithms: introduction to design paradigms*. Texts in theoretical computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 3-540-23949-9. xii + 274 pp. LCCN QA274 .H76 2005.

Hromkovic:2009:AAH

[Hro09] Juraj Hromkovic. *Algorithmic adventures: from knowledge to magic*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 3-540-85986-1. xiii + 363 pp. LCCN QA76.9.A43 H76 2009. URL http://site.ebrary.com/lib/upcatalunya/docDetail.action?docID=10313472.

Haneberg:2002:MSS

[HRS02] Dominik Haneberg, Wolfgang Reif, and Kurt Stenzel. A method for secure Smartcard applications. *Lecture Notes in Computer Science*, 2422:319–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2422/24220319.htm; http://link.springer-ny.com/link/service/series/0558/papers/2422/24220319.pdf.

Hemaspaandra:2008:EDA

[HRS08] Lane A. Hemaspaandra, Jörg Rothe, and Amitabh Saxena. Enforcing and defying associativity, commutativity, totality, and strong noninvertibility for worst-case one-way functions. *Theoretical Computer Science*, 401(1–3):27–

35, July 23, 2008. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Hirt:2000:ERF

[HS00] Martin Hirt and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 539–556. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070539.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070539.pdf`.

Hinsley:2001:CIS

[HS01a] F. H. (Francis Harry) Hinsley and Alan Stripp, editors. *Codebreakers: the inside story of Bletchley Park*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2001. ISBN 0-19-280132-5. xxi + 321 + 8 pp. LCCN D810.C88 C63 2001.

Hoffstein:2001:MAD

[HS01b] Jeffrey Hoffstein and Joseph H. Silverman. MiniPASS: Authentication and digital signatures in a constrained environment. *Lecture Notes in Computer Science*, 1965: 328–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650328.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650328.pdf`.

Halevy:2002:LBE

[HS02a] Dani Halevy and Adi Shamir. The LSD broadcast encryption scheme. In Yung [Yun02a], pages 47–60. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL `http://link.springer.de/link/service/series/0558/bibs/2442/24420047.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420047.pdf`.

Han:2002:HEF

[HS02b] Guo Ping Han and Kai Quan Shi. Half-encryption and full-encryption of fuzzy recognition. *J. Fuzzy Math.*, 10(2):385–397, 2002. ISSN 1066-8950.

Hwang:2007:PEA

[HS07] Ren-Junn Hwang and Sheng-Hua Shiau. Provably efficient authenticated key agreement protocol for multi-servers. *The Computer Journal*, 50(5):602–615, September 2007. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/50/5/602; http://comjnl.oxfordjournals.org/cgi/content/full/50/5/602; http://comjnl.oxfordjournals.org/cgi/reprint/50/5/602.

He:2005:MCP

[HSD+05] Changhua He, Mukund Sundararajan, Anupam Datta, Ante Derek, and John C. Mitchell. A modular correctness proof of IEEE 802.11i and TLS. In Meadows and Syverson [MS05b], pages 2–15. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Hong:2001:KIA

[HSH+01] Deukjo Hong, Jaechul Sung, Seokhie Hong, Wonil Lee, Sangjin Lee, Jongin Lim, and Okyeon Yi. Known-IV attacks on triple modes of operation of block ciphers. *Lecture Notes in Computer Science*, 2248: 208–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480208.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480208.pdf.

Halderman:2008:LWRa

[HSH+08a] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: Cold boot attacks on encryption keys. Technical report, Princeton University, Princeton, NJ, USA, February 21, 2008. 22 pp. URL http://citp.princeton.edu.nyud.net/pub/coldboot.pdf.

Halderman:2008:LWRb

[HSH+08b] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: cold-boot attacks on encryption keys. In ????, editor, *Usenix Security*, page ?? USENIX, Berkeley, CA, USA, 2008. ISBN ???? LCCN ???? URL ????.

Halderman:2009:LWR

[HSH+09] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: cold-boot attacks on encryption keys. *Communications of the Association for Computing Machinery*, 52(5):91–98, May 2009. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Hanaoka:2002:USA

[HSHI02] Goichiro Hanaoka, Junji Shikata, Yumiko Hanaoka, and Hideki Imai. Unconditionally secure anonymous encryption and group authentication. *Lecture Notes in Computer Science*, 2501: 81–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010081.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010081.pdf.

Hanaoka:2006:USA

[HSHI06] Goichiro Hanaoka, Junji Shikata, Yumiko Hanaoka, and Hideki Imai. Unconditionally secure anonymous encryption and group authentication. *The Computer Journal*, 49(3):310–321, May 2006. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/49/3/310; http://comjnl.oxfordjournals.org/cgi/content/full/49/3/310; http://comjnl.oxfordjournals.org/cgi/reprint/49/3/310.

Hernandez:2002:GCT

[HSIR02] Julio César Hernández, José María Sierra, Pedro Isasi, and Arturo Ribagorda. Genetic cryptoanalysis of two rounds TEA. *Lecture Notes in Computer Science*, 2331: 1024–1031, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/0pa8nj982jewn9ev/.

Hwang:2001:LCT

[HSKC01] Ren-Junn Hwang, Timothy K. Shih, Chuan-Ho Kao, and Tsung-Ming Chang. Lossy compression tolerant steganography. *Lecture Notes in Computer Science*, 2105:427–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2105/21050427.htm; http://link.springer-ny.com/link/service/series/0558/papers/2105/21050427.pdf.

Hong:2002:PSR

[HSL+02] Seokhie Hong, Jaechul Sung, Sangjin Lee, Jongin Lim, and Jongsu Kim. Provable security for 13 round Skipjack-like structure. *Information Processing Letters*, 82(5):243–246, June 15, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hong:2002:IDC

[HSM+02] Deukjo Hong, Jaechul Sung, Shiho Moriai, SangjinLee, and Jongin Lim. Impossible differential cryptanalysis of Zodiac. *Lecture Notes in Computer Science*, 2355:300–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550300.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550300.pdf`.

Hernandez:2001:DTR

[HSR+01] Julio César Hernández, José María Sierra, Arturo Ribagorda, Benjamín Ramos, and J. C. Mex-Perera. Distinguishing TEA from a random permutation: Reduced round versions of TEA do not have the SAC or do not generate random numbers. *Lecture Notes in Computer Science*, 2260:374–377, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600374.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600374.pdf`.

Hess:2001:TTH

[HSS01] Florian Hess, Gadiel Seroussi, and Nigel P. Smart. Two topics in hyperelliptic cryptography. *Lecture Notes in Computer Science*, 2259:181–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590181.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590181.pdf`.

Hernandez:2004:STN

[HSS04] Julio C. Hernandez, José María Sierra, and Andre Seznec. The SAC test: a new randomness test, with some applications to PRNG analysis. *Lecture Notes in Computer Science*, 2004:960–967, 2004. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http:`

//www.springerlink.com/content/an44921nlaa5bf0g/.

Hsu:2005:CIT

[Hsu05a] Chien-Lung Hsu. Cryptanalysis and improvement of the Tzeng–Hwang authenticated encryption scheme based on elliptic curve discrete logarithm problem. *Applied Mathematics and Computation*, 167(2):882–890, August 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hsu:2005:UFR

[Hsu05b] Chien-Lung Hsu. A user friendly remote authentication scheme with smart cards against impersonation attacks. *Applied Mathematics and Computation*, 170 (1):135–143, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hasan:2009:PHF

[HSW09] Ragib Hasan, Radu Sion, and Marianne Winslett. Preventing history forgery with secure provenance. *ACM Transactions on Storage*, 5(4):12:1–12:??, December 2009. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Hanaoka:2000:USD

[HSZI00] Goichiro Hanaoka, Junji Shikata, Yuliang Zheng, and Hideki Imai. Unconditionally secure digital signature schemes admitting transferability. *Lecture Notes in Computer Science*, 1976:130–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760130.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760130.pdf.

Hanaoka:2001:EUS

[HSZI01] Goichiro Hanaoka, Junji Shikata, Yuliang Zheng, and Hideki Imai. Efficient and unconditionally secure digital signatures and a security analysis of a multireceiver authentication code. *Lecture Notes in Computer Science*, 2274:64–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740064.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740064.pdf.

Halpern:2004:RSS

[HT04] Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation: extended abstract. In ACM [ACM04b], pages 623–632. ISBN 1-58113-852-0. LCCN QA75.5 .A22 2004.

Huang:2006:CSV

[HT06] Biao-Bing Huang and Shao-Xian Tang. A contrast-sensitive visible watermarking scheme. *IEEE MultiMedia*, 13(2):60–66, April/June 2006. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Hongfeng:2008:ECP

[HTJ08] Zhu Hongfeng, Liu Tianhua, and Liu Jie. EV-C2C-PAKE: An improved client-to-client password-authenticated key exchange protocol. *International Journal of Computer Systems Science and Engineering*, 23(3):??, May 2008. CODEN CSSEEI. ISSN 0267-6192.

Hamalainen:2002:GPS

[HTS02] Antti Hämäläinen, Matti Tommiska, and Jorma Skyttä. 6.78 gigabits per second implementation of the IDEA cryptographic algorithm. *Lecture Notes in Computer Science*, 2438: 760–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2438/24380760.htm; http://link.springer-ny.com/link/service/series/0558/papers/2438/24380760.pdf.

Hines:2007:AIF

[HTW07] Stephen Roderick Hines, Gary Tyson, and David Whalley. Addressing instruction fetch bottlenecks by using an instruction register file. *ACM SIGPLAN Notices*, 42(7):165–174, July 2007. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Hofheinz:2005:CTN

[HU05] Dennis Hofheinz and Dominique Unruh. Comparing two notions of simulatability. In Kilian [Kil05], pages 86–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Hughes:2002:LAA

[Hug02] James Hughes. A linear algebraic attack on the AAFG1 braid group cryptosystem. *Lecture Notes in Computer Science*, 2384:

176–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840176.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840176.pdf.

Hughes:2004:ISE

[Hug04] Jim Hughes. IEEE standard for encrypted storage. *Computer*, 37(11):110–??, November 2004. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/dl/mags/co/2004/11/ry110.htm; http://csdl.computer.org/dl/mags/co/2004/11/ry110.pdf.

Huhnlein:2000:EIC

[Hüh00] Detlef Hühnlein. Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders. *Lecture Notes in Computer Science*, 1758: 147–162, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hunt:2005:JFE

[Hun05] K. Hunt. A Java framework for experimentation with steganography. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 37(1): 282–286, 2005. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Husemann:2001:SSC

[Hus01] Dirk Husemann. Standards in the smart card world. *Computer Networks (Amsterdam, Netherlands: 1999)*, 36(4):473–487, July 16, 2001. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.elsevier.nl/gej-ng/10/15/22/61/28/32/abstract.html; http://www.elsevier.nl/gej-ng/10/15/22/61/28/32/article.pdf.

Husemoller:2004:EC

[Hus04] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2004. ISBN 0-387-95490-2. xxi + 487 pp. LCCN QA567 .H897 2004. URL http://www.loc.gov/catdir/enhancements/fy0814/2002067016-d.html; http://www.loc.gov/catdir/enhancements/fy0814/2002067016-t.html. With appendices by Stefan Theisen, Otto Forster, and Ruth Lawrence.

Huth:2001:SCS

[Hut01] Michael R. A. Huth. *Secure communicating systems: design, analysis, and implementation*. Cambridge University Press, Cambridge, UK, 2001. ISBN 0-521-80731-X (hardcover). x + 283 pp. LCCN TK5102.85 .H88 2001. US$40.00.

Hodjat:2004:HTP

[HV04] Alireza Hodjat and Ingrid Verbauwhede. High-throughput programmable cryptocoprocessor. *IEEE Micro*, 24(3):34–45, May/June 2004. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://csdl.computer.org/dl/mags/mi/2004/03/m3034.htm; http://csdl.computer.org/dl/mags/mi/2004/03/m3034.pdf.

Hallgren:2009:QC

[HV09] Sean Hallgren and Ulrich Vollmer. Quantum computing. In Bernstein et al. [BBD09], pages 15–34. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Hopper:2009:PSS

[HvAL09] N. Hopper, L. von Ahn, and J. Langford. Provably secure steganography. *IEEE Transactions on Computers*, 58(5):662–676, May 2009. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4663056.

Hardy:1998:ITN

[HW98] G. H. (Godfrey Harold) Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. Oxford science publications. Clarendon Press, Oxford, UK, fifth edition, 1998. ISBN 0-19-853171-0 (paperback). xvi + 426 pp. LCCN QA241 .H28 1998.

Hutchinson:2001:IWC

[HW01] William Hutchinson and Matthew Warren. *Information Warfare: Corporate Attack and Defense in a Digital World*. Computer Weekly professional series. Butterworth-Heinemann, Boston, MA, USA, 2001. ISBN 0-7506-4944-5. xx + 204 pp. LCCN QA76.9.A25 H88 2001. US$39.95.

Hardy:2003:AAC

[HW03a] Darel W. Hardy and Carol L. Walker. *Applied algebra: codes, ciphers, and discrete algorithms*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 2003. ISBN 0-13-067464-8. x + 420 pp. LCCN QA268 .H365 2003.

Hellekalek:2003:EEC

[HW03b] Peter Hellekalek and Stefan Wegenkittl. Empirical evidence concerning AES. *ACM Transactions on Modeling and Computer Simulation*, 13(4):322–333, October 2003. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). URL `http://random.mat.sbg.ac.at/ftp/pub/publications/peter/aes_sub.ps`; `http://random.mat.sbg.ac.at/~peter/slides_YACC04.pdf`.

Hsu:2003:CIT

[HW03c] Chien-Lung Hsu and Tzong-Sun Wu. Cryptanalyses and improvements of two cryptographic key assignment schemes for dynamic access control in a user hierarchy. *Computers & Security*, 22(5):453–456, July 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404803005145`.

Hsu:2004:EPS

[HW04] Chien-Lung Hsu and Tzong-Sun Wu. Efficient proxy signature schemes using self-certified public keys. *Applied Mathematics and Computation*, 152(3):807–820, May 13, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hsu:2005:SCT

[HW05] Chien-Lung Hsu and Tzong-Sun Wu. Self-certified threshold proxy signature schemes with message recovery, nonrepudiation, and traceability. *Applied Mathematics and Computation*, 164(1):201–225, May 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hwang:2000:CYK

[Hwa00] Min-Shiang Hwang. Cryptanalysis of YCN key assignment scheme in a hierarchy. *Information Processing Letters*, 73(3-4):97–101, 2000. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:2005:ITA

[Hwa05] Shin-Jia Hwang. Improvement of Tseng et al.'s authenticated encryption scheme. *Applied Mathematics and Computation*, 165(1):1–4, June 6, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Henderson:2001:IEV

[HWH01] Neil J. Henderson, Neil M. White, and Pieter H. Hartel. iButton enrolment and verification requirements for the pressure sequence smartcard biometric. *Lecture Notes in Computer Science*,

2140:124–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400124.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400124.pdf.

Hsu:2005:NPM

[HWH05] Chien-Lung Hsu, Tzong-Sun Wu, and Wei-Hua He. New proxy multi-signature scheme. *Applied Mathematics and Computation*, 162 (3):1201–1206, March 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hu:2008:NNP

[HWH08] Yupu Hu, Baocang Wang, and Wencai He. NTRUSign with a new perturbation. *IEEE Transactions on Information Theory*, 54(7): 3216–3221, July 2008. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Hardy:2009:AAC

[HWR09] Darel W. Hardy, Carol L. Walker, and Fred Richman. *Applied algebra: codes, ciphers, and discrete algorithms*. Discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, second edition, 2009. ISBN 1-4200-7142-4 (hardcover). 410 pp. LCCN QA268 .H365 2009.

Hsu:2002:IGT

[HWW02] Chien-Lung Hsu, Tzong-Sun Wu, and Tzong-Chen Wu. Improvements of generalization of threshold signature and authenticated encryption for group communications. *Information Processing Letters*, 81(1):41–45, January 16, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.com/gej-ng/10/23/20/85/27/33/abstract.html.

Hsu:2003:ITP

[HWW03] Chien-Lung Hsu, Tzong-Sun Wu, and Tzong-Chen Wu. Improvement of threshold proxy signature scheme. *Applied Mathematics and Computation*, 136(2–3):315–321, March 15, 2003. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hsu:2004:GOS

[HWW04] Chien-Lung Hsu, Tzong-Sun Wu, and Tzong-Chen Wu. Group-oriented signature scheme with distinguished signing authorities. *Future Generation Computer Systems*, 20(5): 865–873, June 15, 2004.

CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Harkins:2005:ESU

[HWW05] Ryan Harkins, Eric Weber, and Andrew Westmeyer. Encryption schemes using finite frames and Hadamard arrays. *Experimental Mathematics*, 14(4): 423–433, ???? 2005. CODEN ???? ISSN 1058-6458 (print), 1944-950X (electronic). URL `http://projecteuclid.org/euclid.em/1136926973`.

Hsu:2003:IMA

[HWWM03] Chien-Lung Hsu, Tzong-Sun Wu, Tzong-Chen Wu, and Chris Mitchell. Improvement of modified authenticated key agreement protocol. *Applied Mathematics and Computation*, 142(2–3):305–308, October 10, 2003. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hirose:2001:UAS

[HY01] Shouichi Hirose and Susumu Yoshida. A user authentication scheme with identity and location privacy. *Lecture Notes in Computer Science*, 2119: 235–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190235.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190235.pdf`.

Hwang:2003:CAL

[HY03] Min-Shiang Hwang and Wei-Pang Yang. Controlling access in large partially ordered hierarchies using cryptographic keys. *The Journal of Systems and Software*, 67(2):99–107, August 15, 2003. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Yeh:2008:STB

[hY08] Jyh haw Yeh. A secure time-bound hierarchical key assignment scheme based on RSA public key cryptosystem. *Information Processing Letters*, 105(4):117–120, February 15, 2008. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:2003:ASM

[HYS03] Min-Shiang Hwang, Chao-Chen Yang, and Cheng-Yeh Shiu. An authentication scheme for mobile satellite communication systems. *Operating Systems Review*, 37(4):42–47, October 2003. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Han:2005:PJIb

[HYZ05a] Yiliang Han, Xiaoyuan Yang, and Jian Zhang. Joint signature and encryption on elliptic curve. In *Proceedings of the 11th Joint International Computer Conference — JICC 2005* [HYZ05b], pages 135–?? ISBN 981-270-153-2. LCCN ???? URL `http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html`.

Han:2005:PJI

[HYZ05b] Yiliang Han, Xiaoyuan Yang, and Jian Zhang, editors. *Proceedings of the 11th Joint International Computer Conference — JICC 2005*. World Scientific Publishing Co., Singapore; Philadelphia, PA, USA; River Edge, NJ, USA, 2005. ISBN 981-270-153-2. LCCN ???? URL `http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html`.

Huang:2005:EMP

[HZSL05] Liusheng Huang, Hong Zhong, Hong Shen, and Yonglong Luo. An efficient multiple-precision division algorithm. In Hong Shen and Koji Nakano, editors, *Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005: 5–8 December 2005, Dalian, China*, pages 971–974. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN 0-7695-2405-2. LCCN QA76.58 .I5752 2005. The authors present an integer-division algorithm that runs three to five times faster than Knuth's 1981 original. However, there is an error in the renormalization algorithm that is corrected in [MN14], while retaining the speedup.

IBM-MARS-Team:2000:MAS

[IBM00] IBM MARS Team. MARS and the AES selection criteria. Technical report, IBM Corporation, San Jose, CA, USA, May 15, 2000. URL `http://www.research.ibm.com/security/final-comments.doc`; `http://www.research.ibm.com/security/final-comments.pdf`; `http://www.research.ibm.com/security/final-comments.ps`.

IEEE:2000:ASF

[IEE00a] IEEE, editor. *41st Annual Symposium on Foundations of Computer Science: proceedings: 12–14 November, 2000, Redondo Beach, California*. IEEE

Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2000. CODEN ASFPDV. ISBN 0-7695-0850-2, 0-7695-0851-0 (case), 0-7695-0852-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 2000. IEEE Computer Society order number PR00850.

IEEE:2000:IPH

[IEE00b] IEEE. The IEEE P1363 home page: Standard specifications for public-key cryptography. World-Wide Web site., 2000. URL `http://grouper.ieee.org/groups/1363/index.html`.

IEEE:2001:ISF

[IEE01a] IEEE, editor. *42nd IEEE Symposium on Foundations of Computer Science: proceedings: October 14–17, 2001, Las Vegas, Nevada, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2001. CODEN ASFPDV. ISBN 0-7695-1390-5, 0-7695-1391-3 (case), 0-7695-1392-1 (microfiche). ISSN 0272-5428. LCCN ????

IEEE:2001:EIW

[IEE01b] IEEE, editor. *Eighth IEEE Workshop on Hot Topics in Operating Systems (HotOS-VIII). May 20–23, 2001, Schloss Elmau, Germany*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2001. ISBN 0-7695-1040-X. US$135.00. URL `http://computer.org/CSPRESS/CATALOG/pr01040.htm`. IEEE catalog number PR01040.

IEEE:2002:PAI

[IEE02] IEEE, editor. *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2002, Vancouver, BC, Canada, 16–19 November 2002*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2002. CODEN ASFPDV. ISBN 0-7695-1822-2. ISSN 0272-5428. LCCN QA267. URL `http://ieeexplore.ieee.org/iel5/8411/26517/01181875.pdf`. IEEE Computer Society Order Number PR01822.

IEEE:2003:PAI

[IEE03] IEEE, editor. *Proceedings: 44th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2003, 11–14 October 2003, Cambridge, Massachusetts*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2003. CODEN ASFPDV.

ISBN 0-7695-2040-5. ISSN 0272-5428. LCCN QA76 .S979 2003. URL http://ieeexplore.ieee.org/iel5/8767/27770/01238173.pdf; http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=8767&conhome=1000292. IEEE Computer Society Order Number PR02040.

IEEE:2004:PAI

[IEE04] IEEE, editor. *Proceedings: 45th Annual IEEE Symposium on Foundations of Computer Science: FOCS 2004, 17–19 October, 2004, Rome, Italy*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2004. CODEN ASFPDV. ISBN 0-7695-2228-9. ISSN 0272-5428. LCCN QA276. URL http://ieeexplore.ieee.org/iel5/9430/29918/01366212.pdf; http://ieeexplore.ieee.org/servlet/opac?punumber=9430. IEEE Computer Society Order Number P2228.

IEEE:2005:AIS

[IEE05a] IEEE, editor. *46th Annual IEEE Symposium on Foundations of Computer Science: FOCS 2005: 23–25 October, 2005, Pittsburgh, Pennsylvania, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN 0-7695-2468-0, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S979 2005. IEEE Computer Society order number P2468.

IEEE:2005:PIS

[IEE05b] IEEE, editor. *Proceedings of the 17th IEEE Symposium on Computer Arithmetic, ARITH-17, June 27–29, 2005, Cape Cod, Massachusetts, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN ???? LCCN ????

IEEE:2006:AIS

[IEE06] IEEE, editor. *47th Annual IEEE Symposium on Foundations of Computer Science: FOCS 2006: 21–24 October, 2006, Berkeley, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2006. ISBN 0-7695-2720-5, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S974 2006. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4031329. IEEE Computer Society Order Number P2720.

IEEE:2007:PAI

[IEE07] IEEE, editor. *Proceedings of the 48th Annual IEEE Symposium on Foundations of*

Computer Science: [FOCS 2007]: October 20–23, 2007, Providence, Rhode Island. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2007. ISBN 0-7695-3010-9. ISSN 0272-5428. LCCN QA76 .S974 2007. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4389466. IEEE Computer Society order number P3010.

IEEE:2008:PAI

[IEE08] IEEE, editor. *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science: October 25–23, 2008, Philadelphia, Pennsylvania, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. ISBN 0-7695-3436-8. ISSN 0272-5428. LCCN QA76 .S95 2008. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4690923. IEEE Computer Society order number P3436.

IEEE:2009:ISI

[IEE09a] IEEE, editor. *ICM '09: 21th [sic] International Conference on Microelectronics (ICM 2009): took place from Dec 19, 2009 to Dec 22, 2009 in Marrakech, Morocco*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. ISBN 1-4244-5814-5, 1-4244-5816-1. LCCN TK7870 2009. URL http://ieeexplore.ieee.org/servlet/opac?punumber=5412667.

IEEE:2009:PAI

[IEE09b] IEEE, editor. *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science: October 25–27, 2009, Atlanta, Georgia, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. ISBN 0-7695-3850-9. LCCN QA76 .S95 2009. IEEE Computer Society order number P3850.

Itoi:2001:SIS

[IFH01] Naomaru Itoi, Tomoko Fukuzawa, and Peter Honeyman. Secure Internet smartcards. *Lecture Notes in Computer Science*, 2041: 73–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2041/20410073.htm; http://link.springer-ny.com/link/service/series/0558/papers/2041/20410073.pdf.

Ifrah:2000:UHN

[Ifr00] Georges Ifrah. *The Universal History of Numbers from Prehistory to the Invention of the Computer*. John Wiley and Sons, Inc., New York, NY, USA, 2000. ISBN 0-471-37568-3. xxii + 633 pp. LCCN QA141.I3713 2000. US$39.95. Translated from the French edition, *Histoire universelle des chiffres*, by David Bellos, E. F. Harding, Sophie Wood, and Ian Monk.

Iglesias:2002:NSB

[Igl02] A. Iglesias. A new scheme based on semiconductor lasers with phase-conjugate feedback for cryptographic communications. *Lecture Notes in Computer Science*, 2510:135–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2510/25100135.htm; http://link.springer.de/link/service/series/0558/papers/2510/25100135.pdf.

Isasi:2004:IAE

[IH04] Pedro Isasi and Julio C. Hernandez. Introduction to the applications of evolutionary computation in computer security and cryptography. *Computational Intelligence*, 20(3):445–449, August 2004. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Bassham:2000:ETA

[III00] Lawrence E. Bassham III. Efficiency testing of ANSI C implementations of round 2 candidate algorithms for the Advanced Encryption Standard. In NIST [NIS00], pages 136–148. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Itoh:2003:PCA

[IIT03] Kouichi Itoh, Tetsuya Izu, and Masahiko Takenaka. A practical countermeasure against address-bit differential power analysis. In Walter et al. [WKP03], pages 382–396. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/

tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Iwata:2000:PAF

[IK00] Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of AES finalists — RC6, Serpent, MARS and Twofish (abstract only). In NIST [NIS00], page 9. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Iwata:2001:PAF

[IK01] Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of the AES finalists — RC6 and Serpent. *Lecture Notes in Computer Science*, 1978: 231–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780231.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780231.pdf.

Impagliazzo:2003:LRA

[IK03] R. Impagliazzo and B. M. Kapron. Logics for reasoning about cryptographic constructions. In IEEE [IEE03], pages 372–383. CODEN ASFPDV. ISBN 0-7695-2040-5. ISSN 0272-5428. LCCN QA76 .S979 2003. URL http://ieeexplore.ieee.org/iel5/8767/27770/01238211.pdf?isnumber=27770&prod=CNF&arnumber=1238211&arSt=+372&ared=+383&arAuthor=Impagliazzo%2C+R.%3B+Kapron%2C+B.M.; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=27770&arnumber=1238211&count=66&index=38. IEEE Computer Society Order Number PR02040.

Impagliazzo:2006:LRA

[IK06] Russell Impagliazzo and Bruce M. Kapron. Logics for reasoning about cryptographic constructions. *Journal of Computer and System Sciences*, 72(2):286–320, March 2006. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S0022000005000929.

Ichikawa:2000:HEA

[IKM00] Tetsuya Ichikawa, Tomomi Kasuya, and Mitsuru Matsui. Hardware evaluation of the AES finalists. In NIST [NIS00], pages 279–285. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Ishai:2003:EOT

[IKNP03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In Boneh [Bon03], pages 145–161. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Ishai:2005:SCC

[IKO05] Yuval Ishai, Eyal Kushilevitz, and Rafail Ostrovsky. Sufficient conditions for collision-resistant hashing. In Kilian [Kil05], pages 445–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Ishai:2006:CA

[IKOS06] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography from anonymity. In IEEE [IEE06], pages 239–248. ISBN 0-7695-2720-5, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S974 2006. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4031329. IEEE Computer Society Order Number P2720.

Ishai:2007:ZKS

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In ACM [ACM07], pages 21–30. ISBN 1-59593-631-9. LCCN QA75.5 .A22 2007.

Ishai:2008:CCC

[IKOS08] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with constant computational overhead. In ACM [ACM08], pages 433–442. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Iyer:2007:TAA

[IKP+07] Ravishankar K. Iyer, Zbigniew Kalbarczyk, Karthik Pattabiraman, William Healey, Wen-Mei W. Hwu, Peter Klemperer, and Reza Farivar. Toward application-aware security and reliability. *IEEE Security & Privacy*, 5(1):57–62, January/February 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Ioannidis:2005:ACN

[IKY05] John Ioannidis, Angelos Keromytis, and Moti Yung, editors. *Applied Cryptography and Network Security: Third International Conference, ACNS 2005, New York, NY, USA, June 7–10, 2005, proceedings*, volume 3531 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-26223-7 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK5102.85 .A26 2005. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3531`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b137093`.

Izmerly:2006:CCA

[IM06] Oleg Izmerly and Tal Mor. Chosen ciphertext attacks on lattice-based public key encryption and modern (non-quantum) cryptography in a quantum environment. *Theoretical Computer Science*, 367(3):308–323, December 1, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Izotov:2001:COC

[IMM01] Boris V. Izotov, Alexander A. Moldovyan, and Nick A. Moldovyan. Controlled operations as a cryptographic primitive. *Lecture Notes in Computer Science*, 2052:230–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2052/20520230.htm; http://link.springer-ny.com/link/service/series/0558/papers/2052/20520230.pdf.

Imrey:2003:BRC

[Imr03] Lee Imrey. Book review: *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* by Simon Singh, Delacorte Press, 2000, $15.00, ISBN 0-385-49532-3. *ACM Queue: Tomorrow's Computing Today*, 1(9):76, December/ January 2003. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Inamori:2002:SPB

[Ina02a] Hitoshi Inamori. Security of practical BB84 quantum key distribution. *Algorithmica*, 34(4):366–371, November 2002. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=34&issue=4&spage=366. Quantum computation and quantum cryptography.

Inamori:2002:SPT

[Ina02b] Hitoshi Inamori. Security of practical time-reversed EPR quantum key distribution. *Algorithmica*, 34(4):340–365, November 2002. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=34&issue=4&spage=340. Quantum computation and quantum cryptography.

Inoue:2005:EST

[Ino05] Koji Inoue. Energy-security tradeoff in a secure cache architecture against buffer overflow attacks. *ACM SIGARCH Computer Architecture News*, 33(1):81–89, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Intel:2000:IIP

[Int00] Intel Corporation. Intel Itanium processor: High performance on security algorithms (RSA decryption kernel). Technical report, Intel Corporation, Santa Clara, CA, USA, 2000. 8 pp. URL http://developer.intel.com/design/ia-64/downloads/itaniumssl_seg_103.htm.

Intel:2003:IRN

[Int03] Intel Corporation. The Intel random number generator. World-Wide Web document., 2003. URL http://developer.intel.com/design/chipsets/rng/docs.htm.

Itkis:2001:FSS

[IR01] Gene Itkis and Leonid Reyzin. Forward-secure signatures with optimal signing and verifying. In Kilian [Kil01a], pages 332–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390332.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390332.pdf.

Itkis:2002:SSB

[IR02] Gene Itkis and Leonid Reyzin. SiBIR: Signer-Base Intrusion-Resilient signatures. In Yung [Yun02a], pages 499–514. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420499.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420499.pdf.

Irwin:2003:BRBb

[Irw03] Robert J. Irwin. Book review: *Coding Theory and Cryptography: the Essentials*, second edition, revised and expanded by D.R. Hankerson, et al. Marcel Dekker, 2000. *ACM SIGACT News*, 34(4):17–21, December 2003. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [HHL+00].

ISO:2004:IIIb

[ISO04] ISO. *ISO/IEC 10118-3:2004: Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*. International Organization for Standardization, Geneva, Switzerland, February 2004. 94 pp. URL http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39876.

ISO:2005:IDM

[ISO05] ISO. *ISO 19005-1:2005, Document management—Electronic document file format for long-term preservation—Part 1: Use of PDF 1.4 (PDF/A-1)*. International Organization for Standardization, Geneva, Switzerland, 2005. URL http://www.aiim.org/documents/standards/ISO_19005-1_(E).doc; http://www.aiim.org/pdf_a/.

Iqbal:2008:CDV

[ISSZ08] Razib Iqbal, Shervin Shirmohammadi, Abdulmotaleb El Saddik, and Jiying Zhao. Compressed-domain video processing for adaptation, encryption, and authentication. *IEEE MultiMedia*, 15(2):38–50, April/June 2008. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Inoue:2008:FAC

[ISTE08] Hiroaki Inoue, Junji Sakai, Sunao Torii, and Masato Edahiro. FIDES: an advanced chip multiprocessor platform for secure next generation mobile terminals. *ACM Transactions on Embedded Computing Systems*, 8(1):1:1–1:??, December 2008. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Ishai:2003:PCS

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Boneh [Bon03], pages 463–481. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Itoi:2000:SCI

[Ito00] Naomaru Itoi. Secure coprocessor integration with Kerberos V5. In USENIX [USE00d], page ?? ISBN 1-880446-18-9. LCCN ???? URL http://www.usenix.org/publications/library/proceedings/sec2000/itoi.html.

Itoi:2001:SCS

[Ito01] Naomaru Itoi. SC-CFS: Smartcard secured cryptographic file system. In USENIX [USE01c], page ?? ISBN 1-880446-18-9, 1-880446-07-3. LCCN QA76.9.A25 U565 2001. URL http://www.usenix.org/publications/library/proceedings/sec01/itoi.html.

Iwami:2008:AIA

[Iwa08] Maki Iwami. An attack on improved algebraic surface public-key cryptosystem (abstract only). *ACM Communications in Computer Algebra*, 42(1–2):71–74, March/June 2008. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Imai:2000:CPC

[IY00] Hideki Imai and Atsuhiro Yamagishi. CRYPTREC Project — cryptographic evaluation project for the Japanese electronic government. *Lecture Notes in Computer Science*, 1976: 399–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760399.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760399.pdf.

Irwin:2005:PAI

[IY05] Keith Irwin and Ting Yu. Preventing attribute information leakage in automated trust negotiation. In Meadows and Syverson [MS05b], pages 36–45. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Iwamoto:2006:SSR

[IY06] Mitsugu Iwamoto and Hirosuke Yamamoto. Strongly secure ramp secret sharing schemes for general access structures. *Information Processing Letters*, 97 (2):52–57, January 31, 2006. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Iwata:2002:NCP

[IYK02] Tetsu Iwata, Tomonobu Yoshino, and Kaoru Kurosawa. Non-cryptographic primitive for pseudorandom permutation. *Lecture Notes in Computer Science*, 2365:149–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650149.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650149.pdf.

Iwata:2003:NCP

[IYK03] Tetsu Iwata, Tomonobu Yoshino, and Kaoru Kurosawa. Non-cryptographic primitive for pseudorandom permutation. *Theoretical Computer Science*, 306(1–3):139–154, September 5, 2003. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Imai:2000:PKC

[IZ00] Hideki Imai and Yuliang Zheng, editors. *Public key cryptography: third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne, Victoria, Australia, January 18–20, 2000: proceedings*, volume 1751 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-66967-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1751.

Judge:2002:WWM

[JA02] Paul Judge and Mostafa Ammar. WHIM: watermarking multicast video with a hierarchy of intermediaries. *Computer Networks (Amsterdam, Netherlands: 1999)*, 39(6):699–712, August 21, 2002. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.elsevier.com/gej-ng/10/15/22/96/53/27/abstract.html`.

Jablon:2001:PAU

[Jab01] David P. Jablon. Password authentication using multiple servers. *Lecture Notes in Computer Science*, 2020:344–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200344.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200344.pdf`.

Jackson:2000:SCQ

[Jac00] Chris Jackson. Smart card questions move from technology to applications. *Railway gazette international*, 156(3):167–168, March 2000.

Jambunathan:2000:CCP

[Jam00] K. Jambunathan. On choice of connection-polynomials for LFSR-based stream ciphers. *Lecture Notes in Computer Science*, 1977: 9–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1977/19770009.htm; http://link.springer-ny.com/link/service/series/0558/papers/1977/19770009.pdf`.

Janczewski:2000:IIS

[Jan00] Lech Janczewski. *Internet and intranet security management: risks and solutions*. Idea Group Pub., Hershey, PA, USA, 2000. ISBN 1-878289-71-3. 302 pp. LCCN TK5105.875.I57 I684 2000. Contents: Pt. I. State of the Art. Ch. 1. Security Risk Assessment and Electronic Commerce: A Cross-Industry Analysis / Jonathan W. Palmer, Jamie Kliewer and Mark Sweat. Ch. 2. Securing the Internet in New Zealand: Threats and Solutions / Jairo A. Gutierrez — Pt. II. Managing Intranet and Internet Security. Ch. 3. Developing Trust for Electronic Commerce / Dieter Fink. Ch. 4. Managing Security Functions Using Security Standards / Lech Janczewski. Ch. 5. Managing Security in the World Wide Web: Architecture, Services and Techniques / Fredj Dridi and Gustaf Neumann — Pt. III. Cryptography and Technical Security Standards. Ch. 6. Cryptography: Protecting Confidentiality, Integrity and Availability of Data / Henry B. Wolfe. Ch. 7. Foundations for Cryptography / Dieter Gollmann. Ch. 8. Developments in Security Mechanism Standards / Chris Mitchell — Pt. IV. Security and the Law. Ch. 9. Electronic Mail, Employee Privacy and the Workplace / Charles Prysby and Nicole Prysby. Ch. 10. Protecting Personal Privacy in Cyberspace: The Limitations of Third Generation Data Protection Laws Such as the New Zealand Privacy Act 1993 / Gehan Gunasekara.

Janeczko:2006:TSH

[Jan06] Paul B. Janeczko. *Top Secret: a Handbook of Codes, Ciphers and Secret Writing.* Candlewick Press, Cambridge, MA, USA, 2006. ISBN 0-439-87560-9. 144 (est.) pp. LCCN ????

Jankowski:2008:BRBb

[Jan08a] Richard Jankowski. Book review: *Privacy on the Line: The Politics of Wiretapping and Encryption*, by Whitfield Diffie and Susan Landau. *ACM SIGACT News*, 39(4):30–32, December 2008. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [DL98, DL07].

Jankvist:2008:TMH

[Jan08b] Uffe Thomas Jankvist. A teaching module on the history of public-key cryptography and RSA. *BSHM Bulletin: Journal of the British Society for the History of Mathematics*, 23 (3):157–168, 2008. CODEN ???? ISSN 1749-8430 (print), 1749-8341 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/17498430802304032`.

Jennewein:2000:FCQ

[JAW+00] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4): 1675–1680, 2000. CODEN RSINAK. ISSN 1089-7623, 0034-6748. URL `http://link.aip.org/link/?RSI/71/1675/1`.

Jones:2005:RDF

[JBR05] Keith J. (Keith John) Jones, Richard Bejtlich, and Curtis W. Rose. *Real Digital Forensics: Computer Security and Incident Response*. Addison-Wesley, Reading, MA, USA, 2005. ISBN 0-321-24069-3 (paperback). xxx + 650 pp. LCCN HV8079.C65 J66 2005.

Johnson:2001:IHS

[JDJ01] Neil F. Johnson, Zoran Duric, and Sushil Jajodia. *Information hiding: steganography and watermarking: attacks and countermeasures*, volume 1 of *Advances in information security*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2001. ISBN 0-7923-7204-2. xx + 137 pp. LCCN QA76.9.A25 J25 2001.

Jeffrey:2008:PAM

[Jef08] David Jeffrey, editor. *Proceedings of the 21st annual meeting of the International Symposium on Symbolic Computation, ISSAC 2008, July 20–23, 2008, Hagenberg, Austria*. ACM Press, New York, NY 10036, USA, 2008. ISBN 1-59593-904-0. LCCN ????

Jennings:2009:SLL

[Jen09] Trevor J. Jennings. SPARK: the Libre language and toolset for high-assurance software engineering. *ACM SIGADA Ada Letters*, 29 (3):9–10, December 2009. CODEN AALEE5. ISSN 1094-3641 (print), 1557-9476 (electronic).

Jaeger:2004:CAA

[JEZ04] Trent Jaeger, Antony Edwards, and Xiaolan Zhang. Consistency analysis of authorization hook placement in the Linux security modules framework. *ACM Transactions on Information and System Security*, 7(2):175–205, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Juels:2001:RKG

[JG01] Ari Juels and Jorge Guajardo. RSA key generation with verifiable randomness. *Lecture Notes in Computer Science*, 2274: 357–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740357.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740357.pdf`.

Johnson:2007:EIS

[JG07] M. Eric Johnson and Eric Goetz. Embedding information security into the organization. *IEEE Security & Privacy*, 5(3):16–24, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Jakobsson:2000:MMS

[JJ00a] Markus Jakobsson and Ari Juels. Mix and match: Secure function evaluation via ciphertexts. *Lecture Notes in Computer Science*, 1976:162–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760162.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760162.pdf.

Jaulmes:2000:CCA

[JJ00b] Éliane Jaulmes and Antoine Joux. A chosen-ciphertext attack against NTRU. In Bellare [Bel00], pages 20–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800020.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800020.pdf.

Jaulmes:2000:NC

[JJ00c] Éliane Jaulmes and Antoine Joux. A NICE cryptanalysis. *Lecture Notes in Computer Science*, 1807:382–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070382.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070382.pdf.

Johansson:2000:FCA

[JJ00d] Thomas Johansson and Fredrik Jönsson. Fast correlation attacks through reconstruction of linear polynomials. In Bellare [Bel00], pages 300–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800300.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800300.pdf.

Jaulmes:2001:CPN

[JJ01] Éliane Jaulmes and Antoine Joux. Cryptanalysis of PKP: a new approach. *Lecture Notes in Computer Science*, 1992:165–172, 2001.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jonsson:2002:FCA

[JJ02] Fredrik Jönsson and Thomas Johansson. A fast correlation attack on LILI-128. *Information Processing Letters*, 81(3):127–132, February 14, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.com/gej-ng/10/23/20/85/34/28/abstract.html.

Jakimoski:2001:ASR

[JK01a] Goce Jakimoski and Ljupčo Kocarev. Analysis of some recently proposed chaos-based encryption algorithms. *Physics Letters A*, 291(6):381–384, 2001. CODEN PYLAAG. ISSN 0375-9601 (print), 1873-2429 (electronic).

Jakimoski:2001:CCB

[JK01b] Goce Jakimoski and Ljupčo Kocarev. Chaos and cryptography: block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, 48(2):163–169, 2001. CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic).

Jakimovski:2002:CS

[JK02a] Goce Jakimovski and Ljupčo Kocarev. Cryptanalysis of SBLH. *Lecture Notes in Computer Science*, 2355: 144–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550144.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550144.pdf.

Jonsson:2002:SRE

[JK02b] Jakob Jonsson and Burton S. Kaliski Jr. On the security of RSA encryption in TLS. *Lecture Notes in Computer Science*, 2442:127–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2442/24420127.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420127.pdf.

Jonsson:2002:SRT

[JK02c] Jakob Jonsson and Burton S. Kaliski, Jr. On the security of RSA encryption in TLS. In Yung [Yun02a], pages 127–142. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http:/

/link.springer.de/link/service/series/0558/bibs/2442/24420017.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420017.pdf.

Jang:2001:BWA

[JKK+01] Yongwon Jang, Intaek Kim, Hwan Il Kang, Kab Il Kim, and Seung-Soo Han. Blind watermarking algorithm using complex block selection method. *Lecture Notes in Computer Science*, 2195:996–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950996.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950996.pdf.

Jung:2001:EMO

[JKRW01] Oliver Jung, Sven Kuhn, Christoph Ruland, and Kai Wollenweber. Enhanced modes of operation for the encryption in high-speed networks and their impact on QoS. *Lecture Notes in Computer Science*, 2119:344–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190344.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190344.pdf.

Jallad:2002:ICC

[JKS02] Kahil Jallad, Jonathan Katz, and Bruce Schneier. Implementation of chosen-ciphertext attacks against PGP and GnuPG. In Lynn Batten and Jennifer Seberry, editors, *Information security and privacy: 7th Australasian conference, ACISP 2002, Melbourne, Australia, July 3–5, 2002: proceedings*, volume 2384, page ?? Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. ISBN 3-540-43861-0. LCCN QA76.9.A25 A278 2002. URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330090.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330090.pdf; http://link.springer-ny.com/link/service/series/0558/tocs/t2384.htm; http://www.counterpane.com/pgp-attack.html.

Jarecki:2000:AST

[JL00] Stanisław Jarecki and Anna Lysyanskaya. Adaptively secure threshold cryptography: Introducing concurrency, removing erasures (extended abstract). *Lecture Notes in Computer Science*, 1807:221–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070221.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070221.pdf.

Joux:2003:IGN

[JL03] Antoine Joux and Reynald Lercier. Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the Gaussian integer method. *Mathematics of Computation*, 72(242):953–967, April 2003. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journal-getitem?pii=S0025-5718-02-01482-5; http://www.ams.org/mcom/2003-72-242/S0025-5718-02-01482-5/S0025-5718-02-01482-5.dvi; http://www.ams.org/mcom/2003-72-242/S0025-5718-02-01482-5/S0025-5718-02-01482-5.pdf; http://www.ams.org/mcom/2003-72-242/S0025-5718-02-01482-5/S0025-5718-02-01482-5.ps; http://www.ams.org/mcom/2003-72-242/S0025-5718-02-01482-5/S0025-5718-02-01482-5.tex.

Juang:2004:FBT

[JL04] Wen-Shenq Juang and Horng-Twu Liaw. Fair blind threshold signatures in wallet with observers. *The Journal of Systems and Software*, 72(1):25–31, June 2004. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Jeong:2008:PKE

[JL08] I. R. Jeong and D. H. Lee. Parallel key exchange. *J.UCS: Journal of Universal Computer Science*, 14 (3):377–396, ???? 2008. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_14_3/parallel_key_exchange.

Lee:2007:RKD

[jLC07] Hyoung joo Lee and Sungzoon Cho. Retraining a keystroke dynamics-based authenticator with impostor patterns. *Computers & Security*, 26(4):300–310, June 2007. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404806002057.

Juang:2001:FBT

[JLL01] W.-S. Juang, C.-L. Lei, and H.-T. Liaw. Fair blind threshold signatures based on discrete logarithm. *International Journal of Computer Systems Science and Engineering*, 16(6):??, November 2001. CODEN CSSEEI. ISSN 0267-6192.

Juang:2002:VMA

[JLL02] Wen-Shenq Juang, Chin-Laung Lei, and Horng-Twu Liaw. A verifiable multi-authority secret election allowing abstention from voting. *The Computer Journal*, 45(6):672–682, ???? 2002. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_06/450672.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_45/Issue_06/pdf/450672.pdf`.

Jakobsson:2003:FMT

[JLMS03] Markus Jakobsson, Tom Leighton, Silvio Micali, and Michael Szydlo. Fractal Merkle tree representation and traversal. In Joye [Joy03b], pages 314–326. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612`.

Johansson:2003:PCI

[JM03] Thomas Johansson and Subhamoy Maitra, editors. *Progress in Cryptology— INDOCRYPT 2003: 4th International Conference on Cryptology in India, New Delhi, India, December 8–10, 2003: Proceedings*, volume 2904 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-20609-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I5535 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2904.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2904`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b94593`.

Jakobsson:2007:DPD

[JM07] Markus Jakobsson and Steven Myers. Delayed password disclosure. *ACM SIGACT News*, 38(3):56–75, September 2007. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL `http:`

//doi.acm.org/10.1145/1324215.1324228.

Jing-mei:2005:CRB

[JmBdXgXm05] Liu Jing-mei, Wei Baodian, Cheng Xiang-guo, and Wang Xin-mei. Cryptanalysis of Rijndael S-box and improvement. *Applied Mathematics and Computation*, 170(2):958–975, November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Joux:2002:BAA

[JMV02] Antoine Joux, Gwenaëlle Martinet, and Frédéric Valette. Blockwise-adaptive attackers: Revisiting the (in)security of some provably secure encryption modes: CBC, GEM, IACBC. In Yung [Yun02a], pages 17–30. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420017.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420017.pdf.

Jao:2009:EGB

[JMV09] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *Journal of Number Theory*, 129(6):1491–1504, June 2009. CODEN JNUTA9. ISSN 0022-314X (print), 1096-1658 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022314X09000213.

Johnson:2000:AFR

[Joh00] Don Johnson. AES and future resiliency: More thoughts and questions. In NIST [NIS00], pages 257–268. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Johansson:2003:FSE

[Joh03] Thomas Johansson, editor. *Fast Software Encryption: 10th International Workshop, FSE 2003, Lund, Sweden, February 24–26, 2003: Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-20449-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F77 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2887.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2887; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b93938.

Johnson:2005:OSV

[Joh05] Thomas K. Johnson. An open-secret voting system. *Computer*, 38(3):100–??, March 2005. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/dl/mags/co/2005/03/r3100.htm; http://csdl.computer.org/dl/mags/co/2005/03/r3100.pdf.

Jolish:2001:EDP

[Jol01] Barak D. Jolish. The encryption debate in plaintext: National security and encryption in the United States and Israel. *Lecture Notes in Computer Science*, 1962:202–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620202.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620202.pdf.

Jones:2008:RAA

[Jon08] Josh Jones. The RSA algorithm (abstract only). *ACM Communications in Computer Algebra*, 42(1–2):74, March/June 2008. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Joux:2002:WTP

[Jou02] Antoine Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. *Lecture Notes in Computer Science*, 2369:20–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2369/23690020.htm; http://link.springer-ny.com/link/service/series/0558/papers/2369/23690020.pdf.

Joux:2004:MIH

[Jou04] Antoine Joux. Multicollisions in iterated hash functions. application to cascaded constructions. In Franklin [Fra04], pages 306–?? CODEN LNCSD9.

ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Joux:2009:AC

[Jou09] Antoine Joux. *Algorithmic Cryptanalysis*. Chapman and Hall/CRC cryptography and network security. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 2009. ISBN 1-4200-7002-9 (hardcover). 501 pp. LCCN QA76.9.A43; QA76.9.A43 J693 2009.

Joyner:2000:CTC

[Joy00] David Joyner, editor. *Coding theory and cryptography: from Enigma and Geheimschreiber to quantum theory*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-66336-3 (softcover), 3-642-59663-0 (e-book). LCCN QA268 .C67 1999. UK£44.50. URL http://frode.home.cern.ch/frode/pubs/cryptoday.pdf. Proceedings of the Conference on Coding Theory, Cryptography and Number Theory held at the U.S. Naval Academy during October 25–26, 1998.

Joye:2003:CPY

[Joy03a] Marc Joye. Cryptanalysis of a pay-as-you-watch system. *Information Processing Letters*, 88(3):119–120, November 15, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Joye:2003:TCC

[Joy03b] Marc Joye, editor. *Topics in cryptology, CT-RSA 2003: the Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13–17, 2003: Proceedings*, volume 2612 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Jakobsson:2002:MAL

[JP02a] Markus Jakobsson and David Pointcheval. Mutual authentication for low-power mobile devices. *Lecture Notes in Computer Science*, 2339:178–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2339/23390178.htm; http://link.springer-ny.com/link/service/series/0558/papers/2339/23390178.pdf.

Jaulmes:2002:SHG

[JP02b] Éliane Jaulmes and Guillaume Poupard. On the security of homage group authentication protocol. *Lecture Notes in Computer Science*, 2339:106–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2339/23390106.htm; http://link.springer-ny.com/link/service/series/0558/papers/2339/23390106.pdf.

Joye:2003:GFA

[JP03] Marc Joye and Pascal Paillier. GCD-free algorithms for computing modular inverses. In Walter et al. [WKP03], pages 243–253. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Jain:2006:TMB

[JP06] A. K. Jain and S. Pankanti. A touch of money [biometric authentication systems]. *IEEE Spectrum*, 43(7):22–27, July 2006. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Jakubowska:2007:MCT

[JP07] Gizela Jakubowska and Wojciech Penczek. Modelling and checking timed authentication of security protocols. *Fundamenta Informaticae*, 79(3–4):363–378, February 2007. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Jiang:2004:FAP

[JPL04] Rui Jiang, Li Pan, and Jian-Hua Li. Further analysis of password authentication schemes based on authentication tests. *Computers & Security*, 23(6):469–477, September 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001038.

Joye:2004:CHE

[JQ04] Marc Joye and Jean-Jacques Quisquater, editors. *Cryptographic Hardware and Embedded Systems— CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11–13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22666-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://link.springer-ny.com/link/service/series/0558/tocs/t3156.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3156; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99451.

Joye:2001:PMA

[JQY01] Marc Joye, Jean-Jacques Quisquater, and Moti Yung. On the power of misbehaving adversaries and security analysis of the original EPOC. *Lecture Notes in Computer Science*, 2020: 208–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200208.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200208.pdf.

Joye:2001:OAD

[JQYY01] Marc Joye, Jean-Jacques Quisquater, Sung-Ming Yen, and Moti Yung. Observability analysis — detecting when improved cryptosystems fail. *Lecture Notes in Computer Science*, 2271:17–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710017.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710017.pdf.

Juric:2006:CPW

[JRB+06] Matjaz B. Juric, Ivan Rozman, Bostjan Brumen, Matjaz Colnaric, and Marjan Hericko. Comparison of performance of Web services, WS-Security, RMI, and RMI–SSL. *The Journal of Systems and Software*, 79(5):689–700, May 2006. CODEN JSSODM. ISSN

0164-1212 (print), 1873-1228 (electronic).

Jin:2001:WCS

[JRFH01] Liang Jin, Shi Ren, Liang Feng, and Gao Zheng Hua. WAP clients and set protocol. *Dr. Dobb's Journal of Software Tools*, 26(6):85, 87–89, 91, June 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Jaworski:2009:RKP

[JRR09] J. Jaworski, M. Ren, and K. Rybarczyk. Random key predistribution for wireless sensor networks using deployment knowledge. *Computing*, 85(1–2):57–76, June 2009. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=85&issue=1&spage=57.

Jain:2009:PQR

[JRS09] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A property of quantum relative entropy with an application to privacy in quantum communication. *Journal of the ACM*, 56(6):33:1–33:32, September 2009. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Jarecki:2005:FSP

[JS05] Stanisław Jarecki and Nitesh Saxena. Further simplifications in proactive RSA signatures. In Kilian [Kil05], pages 510–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Jongkook:2001:NUS

[JSJK01] Lee Jongkook, Ryu Shiryong, Kim Jeungseop, and Yoo Keeyoung. A new undeniable signature scheme using smart cards. *Lecture Notes in Computer Science*, 2260:387–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600387.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600387.pdf.

Jiang:2005:SAI

[JSW05] Zhengtao Jiang, Xi Sun, and Yumin Wang. Security analysis and improvement of a double-trapdoor encryption scheme. *Applied Mathematics and Computation*, 169 (1):41–50, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Joye:2001:PAD

[JT01a] M. Joye and C. Tymen. Protections against differential analysis for elliptic curve cryptography. *Lecture Notes in Computer Science*, 2162:377–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620377.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620377.pdf.

Joye:2001:CEN

[JT01b] Marc Joye and Christophe Tymen. Compact encoding of non-adjacent forms with applications to elliptic curve cryptography. *Lecture Notes in Computer Science*, 1992:353–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920353.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920353.pdf.

Joglekar:2005:PEM

[JT05] S. P. Joglekar and S. R. Tate. ProtoMon: Embedded monitors for cryptographic protocol intrusion detection and prevention. *J.UCS: Journal of Universal Computer Science*, 11(1):83–??, January 28, 2005. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_11_1/protomon_embedded_monitors_for.

Juang:2004:EPA

[Jua04] Wen-Shenq Juang. Efficient password authenticated key agreement using smart cards. *Computers & Security*, 23(2):167–173, March 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804000252.

Juels:2004:FCI

[Jue04] Ari Juels, editor. *Financial Cryptography: 8th International Conference, FC 2004, Key West, FL, USA, February 9–12, 2004: Revised Papers*, volume 3110 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-

22420-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 2004. URL http://link.springer-ny.com/link/service/series/0558/tocs/t3110.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3110; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b98935.

Junod:2005:SCB

[Jun05] Pascal Junod. *Statistical cryptanalysis of block ciphers*. Thèse sciences, Faculté Informatique et communications IC, Section des systèmes de communication (Institut de systèmes de communication), EPF Lausanne, Lausanne, Switzerland, 2005. 267 pp. URL http://library.epfl.ch/theses/?nr=3179.

Jutla:2001:EMA

[Jut01] Charanjit S. Jutla. Encryption modes with almost free message integrity. In *Advances in cryptology— EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 529–544. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450529.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450529.pdf.

Ji:2001:CAF

[JW01] Dongyao Ji and Yuming Wang. Comments on *"An approach to the formal verification of the two-party cryptographic protocols"* by Zhang, Li and Xiao. *Operating Systems Review*, 35(1): 6–7, January 2001. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic). See [ZLX99].

Juels:2005:APD

[JW05] Ari Juels and Stephen A. Weis. Authenticating pervasive devices with human protocols. In Shoup [Sho05a], pages 293–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Jeng:2006:EKM

[JW06] Fuh-Gwo Jeng and Chung-Ming Wang. An efficient key-management scheme for hierarchical access control based on elliptic curve cryptosystem. *The Journal of*

Systems and Software, 79 (8):1161–1167, August 2006. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Jin:2005:EAW

[JX05] Cong Jin and Kaihua Xu. Estimation and application of the watermark embedding strength. In Han et al. [HYZ05b], pages 147–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Jiang:2005:RNP

[JXW05] Zhengtao Jiang, Mingsen Xiang, and Yumin Wang. A research on new public-key encryption schemes. *Applied Mathematics and Computation*, 169(1):51–61, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Joye:2001:NMM

[JY01] Marc Joye and Sung-Ming Yen. New minimal modified radix-r representation with applications to smart cards. *Lecture Notes in Computer Science*, 2274: 375–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740375.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740375.pdf.

Jakobsson:2004:ACN

[JYZ04] Markus Jakobsson, Moti Yung, and Jianying Zhou, editors. *Applied Cryptography and Network Security: Second International Conference, ACNS 2004, Yellow Mountain, China, June 8–11, 2004: Proceedings*, volume 3089 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22217-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK5102.94 .A28 2004. URL http://link.springer-ny.com/link/service/series/0558/tocs/t3089.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3089; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b98360.

Jain:2009:NBC

[JZ09] Rahul Jain and Shengyu Zhang. New bounds on classical and quantum one-way communication complexity. *Theoretical Computer Science*, 410(26):2463–2477, June 6, 2009. CODEN

TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Jiang:2005:TMD

[JZCW05] Zhengtao Jiang, Yang Zhan, Dan Chen, and Yumin Wang. Two methods of directly constructing probabilistic public-key encryption primitives based on third-order LFSR sequences. *Applied Mathematics and Computation*, 171 (2):900–911, December 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Kamel:2009:RSW

[KA09] Ibrahim Kamel and Qutaiba Albluwi. A robust software watermarking for copyright protection. *Computers & Security*, 28(6):395–409, September 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S016740480900008X`.

Kadrich:2007:ES

[Kad07] Mark Kadrich. *Endpoint security*. Addison Wesley Professional, Indianapolis, IN, USA, 2007. ISBN 0-321-43695-4 (paperback). ???? pp. LCCN QA76.9.A25 K325 2007.

Kahn:1967:CSSa

[Kah67a] David Kahn. *The Codebreakers: the Story of Secret Writing*. MacMillan Publishing Company, New York, NY, USA, 1967. xvi + 1164 pp. LCCN Z103 .K28. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1000.html`.

Kahn:1967:CSSb

[Kah67b] David Kahn. *The Codebreakers: the Story of Secret Writing*. Weidenfeld and Nicolson, London, UK, 1967. xvi + 1164 pp. LCCN Z103 .K28 1967.

Kahn:1974:C

[Kah74] David Kahn. *The Codebreakers*. Weidenfeld and Nicolson, London, UK, abridged edition, 1974. ISBN 0-297-76785-2. xvi + 576 pp. LCCN Z103 .K28 1974.

Kahn:1996:CSS

[Kah96] David Kahn. *The Codebreakers: the Story of Secret Writing*. Scribner, New York, NY, USA, revised edition, 1996. ISBN 0-684-83130-9. xviii + 1181 pp. LCCN Z103 .K28 1996. See [Tuc66].

Kak:2006:TSQ

[Kak06] Subhash Kak. A three-stage quantum cryptography protocol. *Foundations of Physics Letters*, 19(3):293–296, June 2006. CODEN FPLEET. ISSN 0894-9875 (print), 1572-9524 (electronic).

Kaliski:2001:RDS

[Kal01] Burton S. Kaliski, Jr. RSA digital signatures. *Dr. Dobb's Journal of Software Tools*, 26(5):30, 32–33, 35–36, May 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Kaliski:2003:TRK

[Kal03] Burton S. Kaliski. TWIRL and RSA key size. Web report, RSA Data Security, Inc., Redwood City, CA, USA, May 6, 2003. URL https://web.archive.org/web/20170417095741/https://www.emc.com/emc-plus/rsa-labs/historical/twirl-and-rsa-key-size.htm.

Kayem:2008:RCK

[KAM08] Anne V. D. M. Kayem, Selim G. Akl, and Patrick Martin. On replacing cryptographic keys in hierarchical key management systems. *Journal of Computer Security*, 16(3):289–309, ???? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kanda:2001:PSE

[Kan01] Masayuki Kanda. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function. *Lecture Notes in Computer Science*, 2012: 324–338, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120324.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120324.pdf.

Kapera:2005:MRP

[Kap05] Zdzisław Jan Kapera. *Marian Rejewski pogromca Enigmy. (Polish) [Marian Rejewski tamer of Enigma]*, volume 2 of *Biblioteczka Enigmy*. Enigma Press, Kraków, Poland, 2005. ISBN 83-86110-60-0. 96 pp. LCCN D810.C88 R455 2005.

Karski:2001:SSS

[Kar01] Jan Karski. *Story of a Secret State*. Houghton-Mifflin, Boston, MA, USA, 2001. ISBN 1-931541-39-6 (hardcover). vi + 391 pp. LCCN D802.P6 K3 2001.

Kariya:2002:GM

[Kar02] S. Kariya. Getting the message. *IEEE Spectrum*, 39(8):56–57, August 2002. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Katzenbeisser:2001:RAR

[Kat01] Stefan Katzenbeisser. *Recent advances in RSA cryp-*

tography, volume 3 of *Advances in information security*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2001. ISBN 0-7923-7438-X. xiii + 140 pp. LCCN QA76.9.A25 K38 2001.

Katos:2005:RTB

[Kat05a] Vasilios Katos. A randomness test for block ciphers. *Applied Mathematics and Computation*, 162(1):29–35, March 4, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Katz:2005:CBR

[Kat05b] Jonathan Katz. Comparative book review: *Cryptography: An Introduction*, by V. V. Yaschenko (American Mathematical Society, 2002); *Cryptanalysis of Number Theoretic Ciphers*, by S. S. Wagstaff, Jr. (Chapman & Hall/CRC Press, 2003); *RSA and Public-Key Cryptography*, by R. A. Mollin (Chapman & Hall/CRC Press, 2003); *Foundations of Cryptography, vol. 1: Basic Tools*, by O. Goldreich, (Cambridge University Press, 2001). *ACM SIGACT News*, 36 (2):14–19, June 2005. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL `http://doi.acm.org/10.1145/1067309.1067316`. See [Gol01b, Wag03, Mol03b].

Kendall:1939:TRS

[KB39] Maurice G. (Maurice George) Kendall and Bernard Babington Smith. *Tables of random sampling numbers*, volume XXIV of *Tracts of computers ...*. Cambridge University Press, Cambridge, UK, 1939. x + 60 pp. LCCN QA47 .T7 no.24.

Kovacich:2000:HTC

[KB00] Gerald L. Kovacich and William C. Boni. *High-technology-crime investigator's handbook: working in the global information environment*. Butterworth-Heinemann, Boston, MA, USA, 2000. ISBN 0-7506-7086-X. xix + 298 pp. LCCN HV8079.C65 K68 2000. US$39.95.

Kiely:2006:SSM

[KB06] Laree Kiely and Terry V. Benzel. Systemic security management. *IEEE Security & Privacy*, 4(6): 74–77, November/December 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Kamvar:2007:DTM

[KB07] Maryam Kamvar and Shumeet Baluja. Deciphering trends in mobile search. *Computer*, 40(8):58–62, August 2007. CODEN CPTRB4. ISSN

0018-9162 (print), 1558-0814 (electronic).

Kim:2009:DCA

[KB09] Jongtack Kim and Saewoong Bahk. Design of certification authority using secret redistribution and multicast routing in wireless mesh networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 53(1):98–109, January 16, 2009. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Kachris:2003:RLB

[KBD03] C. Kachris, N. Bourbakis, and A. Dollas. A reconfigurable logic-based processor for the SCAN image and video encryption algorithm. *International Journal of Parallel Programming*, 31(6):489–506, December 2003. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4773/37/6/abstract.htm`; `http://ipsapp007.kluweronline.com/content/getfile/4773/37/6/fulltext.pdf`; `http://www.springerlink.com/openurl.asp?genre=article&issn=0885-7458&volume=31&issue=6&spage=489`.

Keller:2009:ECC

[KBM09] Maurice Keller, Andrew Byrne, and William P. Marnane. Elliptic curve cryptography on FPGA for low-power applications. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 2(1):2:1–2:??, March 2009. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

claffy:2001:IMM

[kc01] kc claffy. Internet measurement: Myths about Internet data, 2001. URL `http://db.usenix.org/publications/library/proceedings/lisa2001/tech/`. Unpublished invited talk, LISA 2001: 15th Systems Administration Conference, December 2–7, 2001, Town and Country Resort Hotel, San Diego, CA.

Kim:2002:SMA

[KC02] Seongyeol Kim and Ilyong Chung. A secure mobile agent system applying identity-based digital signature scheme. *Lecture Notes in Computer Science*, 2510: 588–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2510/25100588.htm`; `http://link.springer.de/link/service/series/0558/papers/2510/25100588.pdf`.

Ku:2005:CFR

[KC05] Wei-Chi Ku and Shuai-Min Chen. Cryptanalysis of a flexible remote user authentication scheme using Smart Cards. *Operating Systems Review*, 39(1):90–96, January 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kieu:2009:HSI

[KC09a] The Duc Kieu and Chin-Chen Chang. A high stego-image quality steganographic scheme with reversibility and high payload using multiple embedding strategy. *The Journal of Systems and Software*, 82(10):1743–1752, October 2009. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Kieu:2009:IAB

[KC09b] The Duc Kieu and Chin-Chen Chang. An image authentication based on discrete Fourier transform. *Fundamenta Informaticae*, 97(4):369–379, December 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Ku:2005:WYR

[KCC05] Wei-Chi Ku, Min-Hung Chiang, and Shen-Tien Chang. Weaknesses of Yoon–Ryu–Yoo's hash-based password authentication scheme. *Operating Systems Review*, 39 (1):85–89, January 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kim:2007:SBE

[KCD07] Jin-Ha Kim, Gyu Sang Choi, and Chita R. Das. An SSL back-end forwarding scheme in cluster-based Web servers. *IEEE Transactions on Parallel and Distributed Systems*, 18(7):946–957, July 2007. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Kim:2001:SAC

[KCJ+01] Seungjoo Kim, Jung Hee Cheon, Marc Joye, Seongan Lim, Masahiro Mambo, Dongho Won, and Yuliang Zheng. Strong adaptive chosen-ciphertext attacks with memory dump (or: The importance of the order of decryption and validation). *Lecture Notes in Computer Science*, 2260:114–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600114.htm`; `http://link.springer-ny.com/link/service/series/`

0558/papers/2260/22600114.pdf.

Ku:2003:WLL

[KCL03] Wei-Chi Ku, Chien-Ming Chen, and Hui-Lung Lee. Weaknesses of Lee–Li–Hwang's hash-based password authentication scheme. *Operating Systems Review*, 37(4):19–25, October 2003. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kang:2001:NHO

[KCP01] Ju-Sung Kang, Seongtaek Chee, and Choonsik Park. A note on the higher order differential attack of block ciphers with two-block structures. *Lecture Notes in Computer Science*, 2015:1–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2015/20150001.htm; http://link.springer-ny.com/link/service/series/0558/papers/2015/20150001.pdf.

Kalker:2004:DWS

[KCR04] Ton Kalker, Ingemar J. Cox, and Yong Man Ro, editors. *Digital Watermarking: Second International Workshop, IWDW 2003, Seoul, Korea, October 20–22, 2003: Revised Papers*, volume 2939 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-21061-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I89 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2939.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2939; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b95658.

Kurosawa:2004:NPH

[KD04] Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In Franklin [Fra04], pages 426–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

King:2001:SAD

[KDO01] Christopher M. King, Curtis E. Dalton, and T. Ertam Osmanoğlu. *Security Ar-*

chitecture: Design, Deployment and Operations. McGraw-Hill, New York, NY, USA, 2001. ISBN 0-07-213385-6. xxii + 481 pp. LCCN QA76.9.A25 K54 2001.

Keefe:2005:CDS

[Kee05] Patrick Radden Keefe. *Chatter: dispatches from the secret world of global eavesdropping*. Random House, New York, NY, USA, 2005. ISBN 1-4000-6034-6. xvii + 300 pp. LCCN JK468.I6 K37 2005. URL http://www.loc.gov/catdir/bios/random051/2004058481.html; http://www.loc.gov/catdir/description/random051/2004058481.html.

Kelsey:2000:KST

[Kel00] J. Kelsey. Key separation in Twofish. Twofish technical report 7, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, April 7, 2000. ???? pp. URL http://www.counterpane.com/twofish-tr7.html.

Kelsey:2002:CIL

[Kel02] John Kelsey. Compression and information leakage of plaintext. *Lecture Notes in Computer Science*, 2365:263–276, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650263.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650263.pdf.

Kellar:2005:NRR

[Kel05a] Sharon S. Kellar. *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 31, 2005. 4 pp. URL http://csrc.nist.gov/cryptval/rng/931rngext.pdf.

Keller:2005:NRR

[Kel05b] Sharon S. Keller. *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 31, 2005. 4 pp. URL http://csrc.nist.gov/cryptval/rng/931rngext.pdf.

Kenyon:2002:DNR

[Ken02a] Tony Kenyon. *Data Networks: Routing, Security, and Performance Optimization*. Digital Press, 12 Crosby Drive, Bedford, MA

01730, USA, 2002. ISBN 1-55558-271-0. xvi + 807 pp. LCCN TK5105.543 .K46 2002. US$59.99.

Kenyon:2002:HPD

[Ken02b] Tony Kenyon. *High Performance Data Network Design: Design Techniques and Tools*. Digital Press, 12 Crosby Drive, Bedford, MA 01730, USA, 2002. ISBN 1-55558-207-9. xiii + 623 pp. LCCN TK5105.5 .K45 2002. US$54.99.

Kettani:2006:CBN

[Ket06] Houssain Kettani. On the conversion between number systems. *IEEE transactions on circuits and systems. 2, Analog and digital signal processing*, 53(11): 1255–1258, November 2006. CODEN ICSPE5. ISSN 1057-7130 (print), 1558-125X (electronic).

Kelsey:2000:CPL

[KFSS00] J. Kelsey, N. Ferguson, B. Schneier, and M. Stay. Cryptanalytic progress: Lessons for AES. In ????, editor, *Third AES Candidate Conference*, page ?? ????, ????, April 2000. ISBN ???? LCCN ????

Kiltz:2009:DCC

[KG09] Eike Kiltz and David Galindo. Direct chosen-ciphertext secure identity-based key encapsulation without random oracles. *Theoretical Computer Science*, 410(47–49):5093–5111, November 6, 2009. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Katsikas:2004:PKI

[KGL04] Sokratis K. Katsikas, Stefanos Gritzalis, and Javier Lopez, editors. *Public Key Infrastructure: First European PKI Workshop: Research and Applications, EuroPKI 2004, Samos Island, Greece, June 25–26, 2004: Proceedings*, volume 3093 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22216-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E973 2004. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t3093.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3093`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b98201`.

Kaps:2007:CSD

[KGS07] Jens-Peter Kaps, Gunnar Gaubatz, and Berk Sunar. Cryptography on a speck of dust. *Computer*, 40(2):38–

44, February 2007. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Kovacich:2003:MHC

[KH03] Gerald L. Kovacich and Edward P. Halibozek. *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann, Boston, MA, USA, 2003. ISBN 0-7506-7487-3. xxi + 463 pp. LCCN HV8290 .K68 2003. US$49.95.

Kim:2005:SMA

[KH05] Byung-Gi Kim and Sang-Sun Hong. Secure mutual authentication for ad hoc wireless networks. *The Journal of Supercomputing*, 33(1):123–132, July 2005. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=33&issue=1&spage=123`.

Kato:2008:QSC

[KH08] Kentaro Kato and Osamu Hirota. A quantum stream cipher by Yuen 2000 protocol with nonlinear random number generator. *Proceedings of the SPIE — The International Society for Optical Engineering*, 7092(1): 70920H, 2008. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/7092/70920H/1`. Quantum Communications and Quantum Imaging VI.

Khaw:2005:EDA

[Kha05] L. T. Khaw. Of encryption and devices: The anticircumvention provision of the Malaysian Copyright Act 1987. *European intellectual property review*, 27 (2):53–64, 2005. ISSN 0142-0461.

Komninos:2001:ESC

[KHD01] N. Komninos, Bahram Honary, and Michael Darnell. An efficient stream cipher Alpha1 for mobile and wireless devices. *Lecture Notes in Computer Science*, 2260:294–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600294.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2260/22600294.pdf`.

Kwon:2005:CLK

[KHKL05] Jeoung Ok Kwon, Jung Yeon Hwang, Changwook Kim, and Dong Hoon Lee. Cryptanalysis of Lee–Kim–Yoo password-based key agreement scheme. *Applied Mathematics and Computation*, 168(2):858–865, September 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Koo:2009:SVN

[KHL09] Woo Kwon Koo, Jung Yeon Hwang, and Dong Hoon Lee. Security vulnerability in a non-interactive ID-based proxy re-encryption scheme. *Information Processing Letters*, 109(23–24): 1260–1262, November 15, 2009. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kirovski:2004:DWF

[KHY04] Darko Kirovski, Henrique, and Yacov Yacobi. A dual watermark-fingerprint system. *IEEE MultiMedia*, 11(3):59–73, July/September 2004. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL `http://csdl.computer.org/dl/mags/mu/2004/03/u3059.htm`; `http://csdl.computer.org/dl/mags/mu/2004/03/u3059.pdf`.

Kausar:2008:SEK

[KHYM08] Firdous Kausar, Sajid Hussain, Laurence T. Yang, and Ashraf Masood. Scalable and efficient key management for heterogeneous sensor networks. *The Journal of Supercomputing*, 45 (1):44–65, July 2008. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=45&issue=1&spage=44`.

Kobara:2001:NCP

[KI01a] Kazukuni Kobara and Hideki Imai. New chosen-plaintext attacks on the one-wayness of the modified McEliece PKC proposed at Asiacrypt 2000. *Lecture Notes in Computer Science*, 2274:237–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740237.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2274/22740237.pdf`.

Kobara:2001:SSM

[KI01b] Kazukuni Kobara and Hideki Imai. Semantically secure McEliece public-key cryptosystems — conversions for McEliece PKC. *Lecture Notes in Computer Science*, 1992:19–35, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920019.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920019.pdf.

Kurosawa:2003:TTK

[KI03] Kaoru Kurosawa and Tetsu Iwata. TMAC: Two-key CBC MAC. In Joye [Joy03b], pages 33–49. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Kidwell:2000:SNC

[Kid00] Peggy A. Kidwell. The Swiss Nema cipher machine [reviews]. *IEEE Annals of the History of Computing*, 22(2):80, April–June 2000. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic).

Kida:2002:PGR

[Kid02] Masanari Kida. Potential good reduction of elliptic curves. *Journal of Symbolic Computation*, 34(3):173–180, September 2002. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Kidwell:2007:CSB

[Kid07] Peggy Aldrich Kidwell. *Colossus: The Secrets of Bletchley Park's Codebreaking Computers* (review). *Technology and Culture*, 48(3):663–664, July 2007. CODEN TECUA3. ISSN 0040-165X (print), 1097-3729 (electronic). URL https://muse.jhu.edu/pub/1/article/218709.

Kilian:2001:ACC

[Kil01a] Joe Kilian, editor. *Advances in cryptology — CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001: proceedings*, volume 2139 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2139.htm.

Kiltz:2001:TBC

[Kil01b] E. Kiltz. A tool box of cryptographic functions related to the Diffie–Hellman function. *Lecture Notes in Computer Science*, 2247:

339–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470339.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470339.pdf.

Kilian:2005:TCS

[Kil05] Joe Kilian, editor. *Theory of cryptography: Second theory of cryptography conference, TCC 2005, Cambridge, MA, USA, February 10–12, 2005, proceedings*, volume 3378 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Kim:2001:PKC

[Kim01] Kwangjo Kim, editor. *Public key cryptography: 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001, Cheju Island, Korea, February 13–15, 2001: Proceedings*, volume 1992 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-41658-7 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I567 2001; QA267.A1 L43 no.1992. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1992.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1992.

Kim:2002:ISC

[Kim02] Kwangjo Kim, editor. *Information security and cryptology — ICISC 2001: 4th International Conference, Seoul, Korea, December 6–7, 2001: Proceedings*, volume 2288 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-43319-8 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I32 2001. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2288.htm; http:

//www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2288.

King:2000:IMP

[Kin00] Brian King. Improved methods to perform threshold RSA. *Lecture Notes in Computer Science*, 1976: 359–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760359.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760359.pdf.

King:2001:CMF

[Kin01] David A. King. *The ciphers of the monks: a forgotten number-notation of the Middle Ages*, volume 44 of *Boethius: Texte und Abhandlungen zur Geschichte der Mathematik der Naturwissenschaften*. F. Steiner, Stuttgart, Germany, 2001. ISBN 3-515-07640-9. 506 pp. LCCN QA141.2 .K56 2001.

King:2002:RGI

[Kin02] Brian King. Requirements for group independent linear threshold secret sharing schemes. *Lecture Notes in Computer Science*, 2384:89–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840089.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840089.pdf.

Kirkby:2001:CCW

[Kir01a] Andrea Kirkby. Cryptography and e-commerce: a Wiley tech brief. *Network Security*, 2001(4):9, April 1, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485801004160.

Kirtland:2001:INC

[Kir01b] Joseph Kirtland. *Identification numbers and check digit schemes*. Classroom resource materials. Mathematical Association of America, Washington, DC, USA, 2001. ISBN 0-88385-720-0. xi + 174 pp. LCCN QA241 .K576 2001. URL http://www.loc.gov/catdir/description/cam021/00108052.html; http://www.loc.gov/catdir/toc/cam027/00108052.html.

Montgomery:2003:FEC

[Kir03] Peter L. Montgomery Kirsten Eisenträger, Kristin Lauter. Fast elliptic curve arithmetic and improved Weil pairing evaluation. In Joye [Joy03b], pages 343–354. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Kocarev:2001:LMB

[KJ01] Ljupčo Kocarev and Goce Jakimoski. Logistic map as a block encryption algorithm. *Physics Letters A*, 289(4-5):199–206, 2001. CODEN PYLAAG. ISSN 0375-9601 (print), 1873-2429 (electronic).

Kanade:2005:AVB

[KJR05] Takeo Kanade, Anil Jain, and Nalini K. Ratha, editors. *Audio- and Video-Based Biometric Person Authentication: 5th International Conference, AVBPA 2005, Hilton Rye Town, NY, USA, July 20–22, 2005. Proceedings*, volume 3546 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-27887-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.S65 I565 2005.

Kim:2005:IYA

[KJY05] Kee-Won Kim, Jun-Cheol Jeon, and Kee-Young Yoo. An improvement on Yang et al.'s password authentication schemes. *Applied Mathematics and Computation*, 170(1):207–215, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Kim:2002:NIS

[KK02] Myungsun Kim and Kwangjo Kim. A new identification scheme based on the bilinear Diffie–Hellman problem. *Lecture Notes in Computer Science*, 2384: 362–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840362.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840362.pdf.

Klein:2003:FOW

[KK03] Andreas Klein and Martin Kutrib. Fast one-way cellular automata. *Theoretical Computer Science*, 295(1–3):233–250, February 24, 2003. CODEN TCSCDI. ISSN 0304-3975

(print), 1879-2294 (electronic).

Kawachi:2006:PQC

[KK06] A. Kawachi and T. Koshiba. Progress in quantum computational cryptography. *J.UCS: Journal of Universal Computer Science*, 12 (6):691–709, ???? 2006. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_12_6/progress_in_quantum_computational.

Kashefi:2007:SZK

[KK07] Elham Kashefi and Iordanis Kerenidis. Statistical Zero Knowledge and quantum one-way functions. *Theoretical Computer Science*, 378 (1):101–116, June 3, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Karri:2003:PBC

[KKG03] Ramesh Karri, Grigori Kuznetsov, and Michael Goessel. Parity-based concurrent error detection of substitution-permutation network block ciphers. In Walter et al. [WKP03], pages 113–124. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Kwon:2003:EEC

[KKH03] Soonhak Kwon, Chang Hoon Kim, and Chun Pyo Hong. Efficient exponentiation for a class of finite fields $GF(2^n)$ determined by Gauss periods. In Walter et al. [WKP03], pages 228–242. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Khachatrian:2001:FMI

[KKIM01] Gurgen H. Khachatrian, Melsik K. Kuregian, Karen R. Ispiryan, and James L. Massey. Fast multiplication of integers for public-key applications. *Lecture Notes in Computer Science*, 2259:245–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:

//link.springer-ny.com/link/service/series/0558/bibs/2259/22590245.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590245.pdf.

Ko:2007:SRT

[KKJ+07] Hoon Ko, Jiyeon Kim, Jongjin Jung, Susan Joe, Yongjun Lee, and Yoonseok Chang. A study on the RFID tag encryption using fast SEED. In Simos and Maroulis [SM07b], pages 571–574. ISBN 0-7354-0476-3 (set), 0-7354-0477-1 (vol. 1), 0-7354-0478-X (vol. 2). ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. LCCN Q183.9 .I524 2007. URL http://proceedings.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf& id=APCPCS000963000002000571000001& idtype=cvips.

Klonowski:2009:SGS

[KKKL09] Marek Klonowski, Lukasz Krzywiecki, Miroslaw Kutylowski, and Anna Lauks. Step-out group signatures. *Computing*, 85(1–2):137–151, June 2009. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=85&issue=1&spage=137.

Kawachi:2005:UTQ

[KKKP05] Akinori Kawachi, Hirotada Kobayashi, Takeshi Koshiba, and Raymond H. Putra. Universal test for quantum one-way permutations. *Theoretical Computer Science*, 345(2–3):370–385, November 22, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Kim:2009:SVN

[KKL09] Soongohn Kim, Seoksoo Kim, and Geuk Lee. Secure verifiable non-interactive oblivious transfer protocol using RSA and bit commitment on distributed environment. *Future Generation Computer Systems*, 25 (3):352–357, March 2009. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Kaliski:2002:CHE

[KKP02] Burton S. Kaliski Jr., Çetin K. Koç, and Christof Paar, editors. *Cryptographic Hardware and Embedded Systems—CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 20. Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-00409-2 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42 C454 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2523.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2523. Also available via the World Wide Web.

Kelsey:2000:ABA

[KKS00a] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent (abstract only). In NIST [NIS00], page 10. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Kohno:2000:PCR

[KKS00b] Tadayoshi Kohno, John Kelsey, and Bruce Schneier. Preliminary cryptanalysis of reduced-round Serpent. In NIST [NIS00], pages 195–214. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Kelsey:2001:ABA

[KKS01] J. Kelsey, T. Kohno, and B. Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Schneier [Sch01d], page ?? CODEN LNCSD9. ISBN 3-540-41728-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no. 1978. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1978.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1978.

Kim:2002:IDS

[KKY02] Nam-Yeun Kim, Dae-Ghon Kho, and Kee-Young Yoo. Inversion/division systolic architecture for public-key cryptosystems in GF(2^m). *Lecture Notes in Computer Science*, 2433: 289–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330289.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330289.pdf.

Katz:2005:HEP

[KL05] Jonathan Katz and Yehuda Lindell. Handling expected polynomial-time strategies in simulation-based security proofs. In Kilian [Kil05], pages 128–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Katz:2008:IMC

[KL08] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography: Principles and Protocols*. Chapman and Hall/CRC cryptography and network security. Chapman and Hall/CRC, Boca Raton, FL, USA, 2008. ISBN 1-58488-551-3. xviii + 534 pp. LCCN QA76.9.A25 K36 2008. URL http://www.loc.gov/catdir/enhancements/fy0807/2007017861-d.html; http://www.loc.gov/catdir/toc/ecip0716/2007017861.html.

Knill:2002:FPE

[KLB+02a] Emanuel Knill, Raymond Laflamme, Howard N. Barnum, Diego A. Dalvit, Jacek J. Dziarmaga, James E. Gubernatis, Leonid Gurvits, Gerardo Ortiz, Lorenza Viola, and Wojciech H. Zurek. From factoring to phase estimation: a discussion of Shor's algorithm. *Los Alamos Science*, 27:38–45, 2002. CODEN LASCDI. ISSN 0273-7116. URL http://library.lanl.gov/cgi-bin/getfile?27-05.pdf.

Knill:2002:QIP

[KLB+02b] Emanuel Knill, Raymond Laflamme, Howard N. Barnum, Diego A. Dalvit, Jacek J. Dziarmaga, James E. Gubernatis, Leonid Gurvits, Gerardo Ortiz, Lorenza Viola, and Wojciech H. Zurek. Quantum information processing: a hands-on primer. *Los Alamos Science*, 27:2–37, 2002. CODEN LASCDI. ISSN 0273-7116. URL http://library.lanl.gov/cgi-bin/getfile?27-07.pdf.

Ko:2000:NPK

[KLC+00] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In Bellare [Bel00], pages 166–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800166.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800166.pdf.

Klein:2007:BDC

[Kle07] Amit Klein. BIND 9 DNS cache poisoning. Report, Trusteer, Ltd., 3 Hayetzira Street, Ramat Gan 52521, Israel, 2007. 21 pp. URL http://www.trusteer.com/docs/BIND_9_DNS_Cache_Poisoning.pdf.

Kong:2001:AVW

[KLL01] Xiangwei Kong, Yu Liu, and Huajian Liu. Adaptive video watermarking scheme. *Lecture Notes in Computer Science*, 2195: 933–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950933.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950933.pdf.

Kiltz:2005:SCM

[KLML05] Eike Kiltz, Gregor Leander, and John Malone-Lee. Secure computation of the mean and related statistics. In Kilian [Kil05], pages 283–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Kacprzak:2006:CBS

[KLN+06] Magdalena Kacprzak, Alessio Lomuscio, Artur Niewiadomski, Wojciech Penczek, Franco Raimondi, and Maciej Szreter. Comparing BDD and SAT based techniques for model checking Chaum's dining cryptographers protocol. *Fundamenta Informaticae*, 72(1–3):215–234, September 2006. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Kalai:2009:SEU

[KLR09] Y. T. Kalai, Xin Li, and A. Rao. 2-source extractors under computational assumptions and cryptography with defective randomness. In IEEE [IEE09b], pages 617–626. ISBN 0-7695-3850-9. LCCN QA76 .S95 2009. IEEE Computer Society order number P3850.

Kim:2002:EPS

[KLY02] Nam-Yeun Kim, Won-Ho Lee, and Kee-Young Yoo. Efficient power-sum systolic architectures for public-key cryptosystems in GF(2^m). *Lecture Notes in Computer Science*, 2387: 153–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2387/23870153.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2387/23870153.pdf`.

Kim:2003:IBP

[KLY03] Hyun-Sung Kim, Sung-Woon Lee, and Kee-Young Yoo. ID-based password authentication scheme using smart cards and fingerprints. *Operating Systems Review*, 37(4):32–41, October 2003. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Knudsen:2000:CRA

[KM00] Lars Knudsen and Willi Meier. Correlations in RC6 (abstract only). In NIST [NIS00], page 9. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf`.

Kim:2001:NPK

[KM01a] Hwankoo Kim and Sang-Jae Moon. New public-key cryptosystem using divisor class groups. *Lecture Notes in Computer Science*, 2119:74–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http:`

//link.springer-ny.com/link/service/series/0558/bibs/2119/21190074.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190074.pdf.

Knudsen:2001:CRR

[KM01b] L. Knudsen and W. Meier. Correlations in RC6 with a reduced number of rounds. In Schneier [Sch01d], page ?? CODEN LNCSD9. ISBN 3-540-41728-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no. 1978. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1978.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1978.

Knudsen:2001:CPL

[KM01c] Lars R. Knudsen and John Erik Mathiassen. A chosen-plaintext linear attack on DES. *Lecture Notes in Computer Science*, 1978:262–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780262.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780262.pdf.

Kanda:2002:SCA

[KM02] Masayuki Kanda and Tsutomu Matsumoto. Security of Camellia against truncated differential cryptanalysis. *Lecture Notes in Computer Science*, 2355:286–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550286.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550286.pdf.

Koblitz:2004:OTS

[KM04a] Neal Koblitz and Alfred J. Menezes. Obstacles to the torsion-subgroup attack on the decision Diffie–Hellman Problem. *Mathematics of Computation*, 73(248):2027–2041, October 2004. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2004-73-248/S0025-5718-04-01637-0/home.html; http://www.ams.org/mcom/2004-73-248/S0025-5718-04-01637-0/S0025-5718-04-01637-0.dvi; http://www.ams.org/mcom/2004-73-248/S0025-5718-04-01637-0/S0025-5718-04-01637-0.pdf; http://www.ams.org/mcom/2004-73-248/S0025-5718-

04-01637-0/S0025-5718-04-01637-0.ps; http://www.ams.org/mcom/2004-73-248/S0025-5718-04-01637-0/S0025-5718-04-01637-0.tex.

Koblitz:2004:SPK

[KM04b] Neal Koblitz and Alfred J. Menezes. A survey of public-key cryptosystems. *SIAM Review*, 46(4):599–634, December 2004. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/43919.

Koblitz:2005:PBC

[KM05] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. Report ??, Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195, USA, May 11, 2005. URL http://www.mathnet.or.kr/mathnet/preprint_file/cacr/2005/cacr2005-08.pdf.

Kornerup:2007:PIS

[KM07] Peter Kornerup and Jean-Michel Muller, editors. *Proceedings of the 18th IEEE Symposium on Computer Arithmetic, June 25–27, 2007, Montpellier, France.* IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2007. ISBN 0-7695-2854-6. ISSN 1063-6889. LCCN ???? URL http://www.lirmm.fr/arith18/.

Kim:2002:ABA

[KML+02] Jongsung Kim, Dukjae Moon, Wonil Lee, Seokhie Hong, Sangjin Lee, and Seokwon Jung. Amplified boomerang attack against reduced-round SHACAL. *Lecture Notes in Computer Science*, 2501: 243–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010243.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010243.pdf.

Kakarountas:2006:HSF

[KMM+06] Athanasios P. Kakarountas, Haralambos Michail, Athanasios Milidonis, Costas E. Goutis, and George Theodoridis. High-speed FPGA implementation of secure hash algorithm for IPSec and VPN applications. *The Journal of Supercomputing*, 37(2):179–195, August 2006. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&

issn=0920-8542&volume=37&issue=2&spage=179.

Katz:2001:CCA

[KMO01] Jonathan Katz, Steven Myers, and Rafail Ostrovsky. Cryptographic counters and applications to electronic voting. *Lecture Notes in Computer Science*, 2045: 78–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450078.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450078.pdf.

Klarlund:2001:MIS

[KMS01] Nils Klarlund, Anders Møller, and Michael I. Schwartzbach. MONA implementation secrets. *Lecture Notes in Computer Science*, 2088:182–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2088/20880182.htm; http://link.springer-ny.com/link/service/series/0558/papers/2088/20880182.pdf.

Klimov:2002:ANC

[KMS02] Alexander Klimov, Anton Mityagin, and Adi Shamir. Analysis of neural cryptography. *Lecture Notes in Computer Science*, 2501: 288–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010288.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010288.pdf.

Keliher:2001:IUB

[KMT01] Liam Keliher, Henk Meijer, and Stafford Tavares. Improving the upper bound on the maximum average linear hull probability for Rijndael. *Lecture Notes in Computer Science*, 2259: 112–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590112.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590112.pdf.

Kim:2003:RCC

[KMZ03] Seungjoo Kim, Masahiro Mambo, and Yuliang Zheng. Rethinking chosen-ciphertext security under Kerckhoffs' assumption. In Joye [Joy03b], pages 227–243. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-

9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Kittler:2003:AVB

[KN03] Josef Kittler and Mark S. Nixon, editors. *Audio-and video-based biometric person authentication: 4th International Conference, AVBPA 2003, Guildford, UK, June 9–11, 2003: Proceedings*, volume 2688 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-40302-7 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.S65 A944 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2688.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2688.

Kol:2008:GEI

[KN08] Gillat Kol and Moni Naor. Games for exchanging information. In ACM [ACM08], pages 423–432. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Koc:2001:CHEb

[KNP01] Çetin K. Koç, David Naccache, and Christof Paar, editors. *Cryptographic hardware and embedded systems — CHES 2001: Third International Workshop, Paris, France, May 14–16, 2001: Proceedings*, volume 2162 of *Lecture Notes in Computer Science and Lecture Notes in Artificial Intelligence*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-42521-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42 C454 2001; QA267.A1 L43 no.2162. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2162.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2162.

Krukow:2005:FCR

[KNS05] Karl Krukow, Mogens Nielsen, and Vladimiro Sassone. A framework for concrete reputation-systems with applications to history-based access control. In Meadows and Syverson [MS05b], pages 260–269. ISBN 1-59593-226-7. LCCN

QA76.9.A25. ACM order number 459050.

Knudsen:2000:TT

[Knu00a] L. Knudsen. Trawling Twofish. Reports in informatics, University of Bergen, Bergen, Norway, April 2000. ???? pp.

Knudsen:2000:TTR

[Knu00b] L. Knudsen. Trawling Twofish — revisited. In ????, editor, *Third AES Candidate Conference*, page ?? ????, ????, April 2000. ISBN ???? LCCN ????

Knudsen:2002:ACE

[Knu02] Lars Knudsen, editor. *Advances in Cryptology— EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28–May 2, 2002. Proceedings*, volume 2332 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-43553-0 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 2002. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2332.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2332`.

Knutson:2007:BPS

[Knu07] Tina R. Knutson. Building privacy into software products and services. *IEEE Security & Privacy*, 5(3):72–74, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Kushilevitz:2000:OWT

[KO00] Eyal Kushilevitz and Rafail Ostrovsky. One-way trapdoor permutations are sufficient for non-trivial single-server private information retrieval. *Lecture Notes in Computer Science*, 1807: 104–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070104.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1807/18070104.pdf`.

Komano:2003:EUP

[KO03] Yuichi Komano and Kazuo Ohta. Efficient universal padding techniques for multiplicative trapdoor one-way permutation. In Boneh [Bon03], pages 366–382. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Katz:2004:ROS

[KO04] Jonathan Katz and Rafail Ostrovsky. Round-optimal secure two-party computation. In Franklin [Fra04], pages 335–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Koblitz:2000:TQC

[Kob00] Neal Koblitz. *Towards a quarter-century of public key cryptography.* Kluwer Academic Publishers, Dordrecht, The Netherlands, 2000. ISBN 0-7923-7802-4. 179 pp. LCCN QA76.9.A25 T69 2000. A special issue of Designs, codes, and cryptography, an international journal, volume 19, no. 2/3 (2000).

Kocher:2002:IS

[Koc02] Paul Kocher. Illusions of security, 2002. URL http://www.usenix.org/publications/library/proceedings/sec02/tech.html. Unpublished.

Koga:2002:GFR

[Kog02] Hiroki Koga. A general formula of the (t, n)-threshold visual secret sharing scheme. *Lecture Notes in Computer Science*, 2501: 328–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010328.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010328.pdf.

Kurosawa:2001:ICP

[KOMM01] Kaoru Kurosawa, Wakaha Ogata, Toshihiko Matsuo, and Shuichi Makishima. IND–CCA public key schemes equivalent to factoring $n = pq$. *Lecture Notes in Computer Science*, 1992:36–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920036.htm;

http://link.springer-ny.com/link/service/series/0558/papers/1992/19920036.pdf.

Kornblum:2009:IBD

[Kor09] Jesse D. Kornblum. Implementing BitLocker drive encryption for forensic analysis. *Digital Investigation*, 5 (3):75–84, ???? 2009. URL ????.

Koshiba:2001:NAS

[Kos01a] Takeshi Koshiba. A new aspect for security notions: Secure randomness in public-key encryption schemes. In *Public key cryptography (Cheju Island, 2001)*, volume 1992 of *Lecture Notes in Comput. Sci.*, pages 87–103. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920087.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920087.pdf.

Koshiba:2001:SRS

[Kos01b] Takeshi Koshiba. On sufficient randomness for secure public-key cryptosystems. *Lecture Notes in Computer Science*, 2274: 34–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740034.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740034.pdf.

Koskinen:2001:NIK

[Kos01c] Jukka A. Koskinen. Non-injective knapsack public-key cryptosystems. *Theoretical Computer Science*, 255(1–2):401–422, March 28, 2001. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.nl../40/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/197/21/40/article.pdf.

Kovach:2001:BCB

[Kov01] Karen Kovach. *Breaking codes, breaking barriers: the WACs of the Signal Security Agency, World War II.* History Office, Office of the Chief of Staff, US Army Intelligence and Security Command, Fort Belvoir, VA, USA, 2001. vi + 49 pp. LCCN UA565.W6 K68 2001.

Kovacich:2003:ISS

[Kov03] Gerald L. Kovacich. *The information systems security officer's guide: establishing and managing* *an information protection program.* Butterworth-Heinemann, Boston, MA, USA, second edition, 2003. ISBN 0-7506-7656-6. xxviii + 361 pp. LCCN QA76.9.A25 K68 2003. US$39.95.

Katz:2001:EPA

[KOY01] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient password-authenticated key exchange using human-memorable passwords. *Lecture Notes in Computer Science*, 2045:475–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450475.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2045/20450475.pdf`.

Katz:2009:ESA

[KOY09] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient and secure authenticated key exchange using weak passwords. *Journal of the ACM*, 57(1):3:1–3:39, November 2009. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Katzenbeisser:2000:IHT

[KP00] Stefan Katzenbeisser and Fabien A. P. Petitcolas, editors. *Information hiding techniques for steganography and digital watermarking.* Artech House computer security series. Artech House Inc., Norwood, MA, USA, 2000. ISBN 1-58053-035-4. xviii + 220 pp. LCCN QA76.9.A25 I54144 2000.

Koc:2001:CHEa

[KP01] Çetin K. Koç and Christof Paar, editors. *Cryptographic hardware and embedded systems — CHES 2000: Second International Workshop, Worcester, MA, USA, August 17–18, 2000: Proceedings*, volume 1965 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-41455-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42 C454 2000. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1965.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1965`.

Koc:2003:GEI

[KP03] C. K. Koc and C. Paar. Guest editors' introduction to the special section on cryptographic hardware and embedded systems. *IEEE Transactions on Computers*, 52(4):401–402, April 2003.

CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1190580.

Kerins:2002:FPE

[KPMF02] Tim Kerins, Emanuel Popovici, William Marnane, and Patrick Fitzpatrick. Fully parameterizable elliptic curve cryptography processor over GF(2). *Lecture Notes in Computer Science*, 2438: 750–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2438/24380750.htm; http://link.springer-ny.com/link/service/series/0558/papers/2438/24380750.pdf.

Klima:2003:ARB

[KPR03] Vlastimil Klíma, Ondrej Pokorný, and Tomáš Rosa. Attacking RSA-based sessions in SSL/TLS. In Walter et al. [WKP03], pages 426–440. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Kaufman:2002:NSP

[KPS02] Charlie Kaufman, Radia Perlman, and Michael Speciner. *Network security: private communication in a public world*. Prentice Hall series in computer networking and distributed systems. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, second edition, 2002. ISBN 0-13-046019-2. xxvi + 713 pp. LCCN QA76.9.A25 K39 2002.

Kim:2004:TBG

[KPT04] Yongdae Kim, Adrian Perrig, and Gene Tsudik. Tree-based group key agreement. *ACM Transactions on Information and System Security*, 7(1):60–96, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Krishna:2003:BUP

[KR03] Shankara Narayanan Krishna and Raghavan Rama. Breaking DES using P systems. *Theoretical Computer Science*, 299(1–3):495–508, April 18, 2003. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Krawczyk:2001:OEA

[Kra01] Hugo Krawczyk. The order of encryption and authentication for protecting communications (or: How secure is SSL?). In Kilian [Kil01a], pages 310–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390310.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390310.pdf.

Krause:2002:BBC

[Kra02a] Matthias Krause. BDD-based cryptanalysis of keystream generators. *Lecture Notes in Computer Science*, 2332: 222–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320222.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320222.pdf.

Krause:2002:USP

[Kra02b] Rory Krause. Using SSH port forwarding to print at remote locations. *Linux Journal*, 94:60–62, 64, February 2002. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://noframes.linuxjournal.com/lj-issues/issue94/article.php?sid=5462.

Krawczy:2003:SSM

[Kra03] Hugo Krawczy. SIGMA: The "SIGn-and-MAc" approach to authenticated Diffie–Hellman and its use in the IKE protocols. In Boneh [Bon03], pages 400–425. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Krawczyk:2005:HHP

[Kra05] Hugo Krawczyk. HMQV: a high-performance secure Diffie–Hellman protocol. In Shoup [Sho05a], pages 546–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http:/

/www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Kramer:2007:LCC

[Kra07] Simon Kramer. Logical concepts in cryptography. *ACM SIGACT News*, 38 (4):65–66, December 2007. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL http://doi.acm.org/10.1145/1345189.1345205.

Kreitz:2005:OBE

[Kre05] Gunnar Kreitz. Optimization of broadcast encryption schemes. Examensarbete, Numerisk analys och datalogi, Kungliga Tekniska högskolan, Stockholm, Sweden, 2005. 61 pp.

Koeune:2002:FIL

[KRS+02] François Koeune, Gael Rouvroy, François-Xavier Standaert, Jean-Jacques Quisquater, Jean-Pierre David, and Jean-Didier Legat. An FPGA implementation of the linear cryptanalysis. *Lecture Notes in Computer Science*, 2438:845–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2438/24380845.htm; http://link.springer-ny.com/link/service/series/0558/papers/2438/24380845.pdf.

Kehr:2001:ISM

[KRV01] Roger Kehr, Michael Rohs, and Harald Vogt. Issues in smartcard middleware. *Lecture Notes in Computer Science*, 2041:90–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2041/20410090.htm; http://link.springer-ny.com/link/service/series/0558/papers/2041/20410090.pdf.

Kim:2005:CLL

[KRY05] Kee-Won Kim, Eun-Kyung Ryu, and Kee-Young Yoo. Cryptanalysis of Lee–Lee authenticated key agreement scheme. *Applied Mathematics and Computation*, 163(1):193–198, April 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Katz:2000:CCA

[KS00a] Jonathan Katz and Bruce Schneier. A chosen ciphertext attack against several E-mail encryption protocols. In USENIX [USE00d], page ?? ISBN 1-880446-18-9. LCCN ???? URL http://www.usenix.org/publications/library/proceedings/sec2000/katz.html.

Kelsey:2000:MAP

[KS00b] John Kelsey and Bruce Schneier. MARS attacks! preliminary cryptanalysis of reduced-round MARS variants. In NIST [NIS00], pages 169–185. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Kuramitsu:2002:ETC

[KS02] K. Kuramitsu and K. Sakamura. Electronic tickets on contactless Smartcard database. *Lecture Notes in Computer Science*, 2453:392–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2453/24530392.htm; http://link.springer-ny.com/link/service/series/0558/papers/2453/24530392.pdf.

Krause:2003:DOC

[KS03] Matthias Krause and Hans Ulrich Simon. Determining the optimal contrast for secret sharing schemes in visual cryptography. *Combinatorics, Probability and Computing*, 12(3):285–299, May 2003. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic). URL http://journals.cambridge.org/action/displayIssue?jid=CPC&volumeId=12&issueId=03. Combinatorics, probability and computing (Oberwolfach, 2001).

Kozaczuk:2004:EHP

[KS04] Władysław Kozaczuk and Jerzy Straszak. *Enigma: how the Poles broke the Nazi code.* Hippocrene Books, New York, NY, USA, 2004. ISBN 0-7818-0941-X. viii + 163 pp. LCCN D810.C88 K67 2004. URL http://www.loc.gov/catdir/toc/fy051/2004040636.html.

Katz:2005:MIA

[KS05a] Jonathan Katz and Ji Sun Shin. Modeling insider attacks on group key-exchange protocols. In Meadows and Syverson [MS05b], pages 180–189. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Kiltz:2005:TCL

[KS05b] Eike Kiltz and Hans Ulrich Simon. Threshold circuit lower bounds on cryptographic functions. *Journal of Computer and System Sciences*, 71(2):185–212, August 2005. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000005000292.

Kissner:2005:PPS

[KS05c] Lea Kissner and Dawn Song. Privacy-preserving set operations. In Shoup [Sho05a], pages 241–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Klivans:2006:CHL

[KS06a] Adam R. Klivans and Alexander A. Sherstov. Cryptographic hardness for learning intersections of halfspaces. In IEEE [IEE06], pages 553–562. ISBN 0-7695-2720-5, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S974 2006. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4031329. IEEE Computer Society Order Number P2720.

Kurkowski:2006:QFF

[KS06b] Mirosław Kurkowski and Marian Srebrny. A quantifier-free first-order knowledge logic of authentication. *Fundamenta Informaticae*, 72 (1–3):263–282, September 2006. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Kasper:2009:FTA

[KS09a] Emilia Käsper and Peter Schwabe. Faster and timing-attack resistant AES–GCM. In ????, editor, *Cryptographic Hardware and Embedded Systems–CHES 2009*, pages 1–17. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN ???? LCCN ???? URL ????.

Klivans:2009:CHL

[KS09b] Adam R. Klivans and Alexander A. Sherstov. Cryptographic hardness for learning intersections of halfspaces. *Journal of Computer and System Sciences*, 75(1):2–12, January 2009. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000008000706.

Kelsey:2000:YND

[KSF00] John Kelsey, Bruce Schneier, and Niels Ferguson. Yarrow-160: Notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator. In Heys and Adams [HA00], pages 13–33. ISBN 3-540-67185-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1758. URL http://www.counterpane.com/yarrow-notes.html; http://www.schneier.com/paper-yarrow.html. Contents: A universal encryption standard / Helena Handschuh and Serge Vaudenay — Yarrow-160: notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator / John Kelsey, Bruce Schneier, and Niels Ferguson — Elliptic curve pseudorandom sequence generators / Guang Gong, Thomas A. Berson, and Douglas R. Stinson — Adaptive-attack norm for decorrelation and super-pseudorandomness / Serge Vaudenay — Guesswork and variation distance as measures of cipher security / John O. Pliam — Modeling linear characteristics of substitution-permutation networks / Liam Keliher, Henk Meijer, and Stafford Tavares — Strong linear dependence and unbiased distribution of non-propagative vectors / Yuliang Zheng and Xian-Mo Zhang — Security of E2 against truncated differential cryptanalysis / Shiho Moriai ... [et al..] — Key-schedule cryptanalysis of DEAL / John Kelsey and Bruce Schneier — Efficient evaluation of security against generalized interpolation attack / Kazumaro Aoki — Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders / Detlef Huhnlein — Improving and extending the Lim/Lee exponentiation algorithm / Biljana Cubaleska, Andreas Rieke, and Thomas Hermann — Software optimization of decorrelation module / Fabrice Noilhan — Pseudonym systems / Anna Lysyanskaya ... [et al.] — Unconditionally secure proactive secret sharing scheme with combinatorial structures / Douglas R. Stinson and R. Wei — Protecting a mobile agent's route against collusions / Dirk Westhoff ... [et al.] — Photuris: design criteria / William Allen Simpson.

Kang:2001:PSK

[KSHY01] Ju-Sung Kang, Sang-Uk Shin, Dowon Hong, and Okyeon Yi. Provable security of KASUMI and 3GPP encryption mode $f8$. *Lecture Notes in Computer Science*, 2248:255–271, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480255.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480255.pdf`.

Kumar:2002:APS

[KSR02] M. V. N. Ashwin Kumar, K. Srinathan, and C. Pandu Rangan. Asynchronous perfectly secure computation tolerating generalized adversaries. *Lecture Notes in Computer Science*, 2384:497–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840497.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840497.pdf`.

Kogan:2006:PRS

[KSW06] Noam Kogan, Yuval Shavitt, and Avishai Wool. A practical revocation scheme for broadcast encryption using smartcards. *ACM Transactions on Information and System Security*, 9(3):325–351, August 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Kelsey:2000:SCC

[KSWH00] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Side channel cryptanalysis of product ciphers. *Journal of Computer Security*, 8(2–3):141–158, ???? 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Konstantinou:2002:SLE

[KSZ02] Elisavet Konstantinou, Yiannis Stamatiou, and Christos Zaroliagis. A software library for elliptic curve cryptography. *Lecture Notes in Computer Science*, 2461:625–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2461/24610625.htm; http://link.springer-ny.com/link/service/series/0558/papers/2461/24610625.pdf`.

Kuribayashi:2000:WSB

[KT00] Minoru Kuribayashi and Hatsukazu Tanaka. A watermarking scheme based on the characteristic of addition among DCT coefficients. *Lecture Notes in Computer Science*, 1975:1–??, 2000. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1975/19750001.pdf.

Kuribayashi:2001:NAF

[KT01] M. Kuribayashi and H. Tanaka. A new anonymous fingerprinting scheme with high enciphering rate. *Lecture Notes in Computer Science*, 2247:30–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470030.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470030.pdf.

Kogan:2006:IER

[KT06] Noam Kogan and Tamir Tassa. Improved efficiency for revocation schemes via Newton interpolation. *ACM Transactions on Information and System Security*, 9(4):461–486, November 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ku:2003:TSA

[KTC03] Wei-Chi Ku, Hao-Chuan Tsai, and Shuai-Min Chen. Two simple attacks on Lin–Shen–Hwang's strong-password authentication protocol. *Operating Systems Review*, 37(4):26–31, October 2003. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kobayashi:2007:AIG

[KTT07] Katsuki Kobayashi, Naofumi Takagi, and Kazuyoshi Takagi. An algorithm for inversion in GF(2^m) suitable for implementation using a polynomial multiply instruction on GF(2). In Kornerup and Muller [KM07], pages 105–112. ISBN 0-7695-2854-6. ISSN 1063-6889. LCCN ???? URL http://www.lirmm.fr/arith18/.

Ku:2002:IIB

[Ku02] Wei-Chi Ku. An improved ID-based authentication and key distribution protocol. *Lecture Notes in Computer Science*, 2344:375–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2344/23440375.htm; http://link.springer.de/link/service/series/0558/papers/2344/23440375.pdf.

Ku:2004:HBS

[Ku04] Wei-Chi Ku. A hash-based strong-password authentication scheme without using Smart Cards. *Operating Systems Review*, 38(1):29–34, January 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kuhn:2000:PCL

[Kuh00] Markus G. Kuhn. Probabilistic counting of large digital signature collections. In USENIX [USE00d], page ?? ISBN 1-880446-18-9. LCCN ???? URL http://www.usenix.org/publications/library/proceedings/sec2000/kuhn.html.

Kuhn:2001:CRR

[Küh01] Ulrich Kühn. Cryptanalysis of reduced-round MISTY. *Lecture Notes in Computer Science*, 2045: 325–329, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kuhn:2002:OTD

[Kuh02a] Markus Kuhn. Optical time-domain eavesdropping risks of CRT displays. In IEEE, editor, *Proceedings: 2002 IEEE Symposium on Security and Privacy, 12-15 May, 2002, Berkeley, California*, pages 3–18. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2002. ISBN 0-7695-1543-6. LCCN QA76.9.A25 I34 2002. URL http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf. IEEE Computer Society Order Number PR01543.

Kuhn:2002:ICM

[Küh02b] Ulrich Kühn. Improved cryptanalysis of MISTY1. *Lecture Notes in Computer Science*, 2365:61–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650061.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650061.pdf.

Kuhn:2008:BSS

[Küh08] Ulrich Kühn. Breaking the Shin–Shin–Rhee remotely keyed encryption schemes. *Information Processing Letters*, 105(6):236–240, March 16, 2008. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kukorelly:2001:PAL

[Kuk01] Zsolt Kukorelly. The piling-up approximation in linear cryptanalysis. *IEEE Transactions on Information Theory*, 47(7):2812–2823, July 2001. CODEN

IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Kumagai:2007:RSK

[Kum07] J. Kumagai. A robotic sentry for Korea's Demilitarized Zone. *IEEE Spectrum*, 44(3):16–17, March 2007. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Kundur:2001:WDI

[Kun01] Deepa Kundur. Watermarking with diversity: Insights and implications. *IEEE MultiMedia*, 8(4):46–52, October 2001. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://dlib.computer.org/mu/books/mu2001/pdf/u4046.pdf; http://www.computer.org/multimedia/mu2001/u4046abs.htm.

Kurosawa:2001:MRP

[Kur01] Kaoru Kurosawa. Multi-recipient public-key encryption with shortened ciphertext. *Lecture Notes in Computer Science*, 2274:48–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740048.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740048.pdf.

Kusters:2002:DCP

[Küs02] Ralf Küsters. On the decidability of cryptographic protocols with open-ended data structures. *Lecture Notes in Computer Science*, 2421:515–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2421/24210515.htm; http://link.springer.de/link/service/series/0558/papers/2421/24210515.pdf.

Kuo:2001:AOS

[KV01] H. Kuo and I. Verbauwhede. Architectural optimization for a 1.82gbits/sec VLSI implementation of the AES Rijndael algorithm. *Lecture Notes in Computer Science*, 2162:51–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620051.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620051.pdf.

Komninos:2007:ALS

[KVD07] Nikos Komninos, Dimitrios D. Vergados, and Christos Douligeris. Authentication in a layered security approach for mobile ad hoc networks. *Computers & Security*, 26(5):373–380, August 2007. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404807000041`.

Kejariwal:2009:ELL

[KVN+09] Arun Kejariwal, Alexander V. Veidenbaum, Alexandru Nicolau, Milind Girkar, Xinmin Tian, and Hideki Saito. On the exploitation of loop-level parallelism in embedded applications. *ACM Transactions on Embedded Computing Systems*, 8(2):10:1–10:??, January 2009. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Koshiba:2000:SEP

[KW00] Takeshi Koshiba and Osamu Watanabe. Strong encryption of public key cryptosystems based on weak randomness hypotheses. *Sūrikaisekikenkyūsho Kōkyūroku*, 1148(1148):118–123, 2000. Theoretical foundations of computer science: toward a paradigm for computing in the 21st century (Japanese) (Kyoto, 2000).

Knudsen:2002:IC

[KW02] Lars Knudsen and David Wagner. Integral cryptanalysis. *Lecture Notes in Computer Science*, 2365: 112–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650112.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2365/23650112.pdf`.

Karlof:2003:HMM

[KW03] Chris Karlof and David Wagner. Hidden Markov model cryptanalysis. In Walter et al. [WKP03], pages 17–34. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240`.

Keromytis:2006:COS

[KWDB06] Angelos D. Keromytis, Jason L. Wright, Theo De Raadt, and Matthew Burnside. Cryptography as an operating system service: a case study. *ACM Transactions on Computer Systems*, 24(1):1–38, February 2006. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Kwon:2002:DSA

[Kwo02] Taekyoung Kwon. Digital signature algorithm for securing digital identities. *Information Processing Letters*, 82(5):247–252, June 15, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See erratum [Kwo03b].

Kwok:2003:WBC

[Kwo03a] Sai Ho Kwok. Watermark-based copyright protection system security. *Communications of the Association for Computing Machinery*, 46(10):98–101, October 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Kwon:2003:EDS

[Kwo03b] Taekyoung Kwon. Erratum to: "Digital signature algorithm for securing digital identities": [Inform. Process. Lett. **82** (2002) 247–252]. *Information Processing Letters*, 88(4):201–202, November 30, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [Kwo02].

Kumar:2006:ODS

[KWP06] Sandeep Kumar, T. Wollinger, and C. Paar. Optimum digit serial GF(2^m) multipliers for curve-based cryptography. *IEEE Transactions on Computers*, 55(10):1306–1311, October 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1683761`.

Wong:2001:MCC

[kWpLwW01] Wai kit Wong, Lap piu Lee, and Kwok wo Wong. A modified chaotic cryptographic method. *Computer Physics Communications*, 138(3):234–236, August 15, 2001. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S001046550100220X`. See comment and reply [ÁMRP04, WLW04].

Kun:2000:SMA

[KXD00] Yang Kun, Guo Xin, and Liu Dayou. Security in mobile agent system: problems and approaches. *Operating Systems Review*, 34(1):21–28, January 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kamat:2009:TPW

[KXTZ09] Pandurang Kamat, Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Temporal privacy in wireless sensor networks: Theory and practice. *ACM Transactions on Sensor Networks*, 5(4):28:1–28:??, November 2009. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Katz:2000:CCS

[KY00] Jonathan Katz and Moti Yung. Complete characterization of security notions for probabilistic private-key encryption. In ACM [ACM00], pages 245–254. ISBN 1-58113-184-4. URL http://www.acm.org/pubs/articles/proceedings/stoc/335305/p245-katz/p245-katz.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/335305/p245-katz/. ACM order number 508000.

Katz:2001:UEC

[KY01a] Jonathan Katz and Moti Yung. Unforgeable encryption and chosen ciphertext secure modes of operation. *Lecture Notes in Computer Science*, 1978: 284–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780284.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780284.pdf.

Kavut:2001:SCP

[KY01b] Selçuk Kavut and Melek D. Yücel. On some cryptographic properties of Rijndael. *Lecture Notes in Computer Science*, 2052: 300–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2052/20520300.htm; http://link.springer-ny.com/link/service/series/0558/papers/2052/20520300.pdf.

Kiayias:2001:PRB

[KY01c] Aggelos Kiayias and Moti Yung. Polynomial reconstruction based cryptography. *Lecture Notes in Computer Science*, 2259: 129–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590129.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590129.pdf.

Kiayias:2001:SPP

[KY01d] Aggelos Kiayias and Moti Yung. Self protecting pirates and black-box traitor tracing. In Kilian [Kil01a], pages 63–?? ISBN 3-540-42456-3 (paperback). LCCN

QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390063.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390063.pdf.

Kurosawa:2001:LCI

[KY01e] Kaoru Kurosawa and Takuya Yoshida. Linear code implies public-key traitor tracing. *Lecture Notes in Computer Science*, 2274: 172–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740172.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740172.pdf.

Katz:2002:TCB

[KY02a] Jonathan Katz and Moti Yung. Threshold cryptosystems based on factoring. *Lecture Notes in Computer Science*, 2501: 192–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010192.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010192.pdf.

Kiayias:2002:CHB

[KY02b] Aggelos Kiayias and Moti Yung. Cryptographic hardness based on the decoding of Reed–Solomon codes. *Lecture Notes in Computer Science*, 2380: 232–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2380/23800232.htm; http://link.springer-ny.com/link/service/series/0558/papers/2380/23800232.pdf.

Kim:2002:PAA

[KY02c] Hyun-Sung Kim and Kee-Young Yoo. Parallel algorithm and architecture for public-key cryptosystem. *Lecture Notes in Computer Science*, 2510: 145–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2510/25100145.htm; http://link.springer.de/link/service/series/0558/papers/2510/25100145.pdf.

Katz:2003:SPA

[KY03] Jonathan Katz and Moti Yung. Scalable protocols for authenticated group key exchange. In Boneh [Bon03], pages 110–125. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Kamal:2009:FIN

[KY09] A. A. Kamal and A. M. Youssef. An FPGA implementation of the NTRUEncrypt cryptosystem. In IEEE [IEE09a], pages 209–?? ISBN 1-4244-5814-5, 1-4244-5816-1. LCCN TK7870 2009. URL http://ieeexplore.ieee.org/servlet/opac?punumber=5412667.

Kang:2001:PMT

[KYHC01] Ju-Sung Kang, Okyeon Yi, Dowon Hong, and Hyunsook Cho. Pseudorandomness of MISTY-type transformations and the block cipher KASUMI. *Lecture Notes in Computer Science*, 2119:60–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190060.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190060.pdf.

Kabatnik:2001:LSD

[KZ01] M. Kabatnik and A. Zugenmaier. Location stamps for digital signatures: a new service for mobile telephone networks. *Lecture Notes in Computer Science*, 2094:20–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2094/20940020.htm; http://link.springer-ny.com/link/service/series/0558/papers/2094/20940020.pdf.

Kamp:2003:DEB

[KZ03] J. Kamp and D. Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. In IEEE [IEE03], pages 92–101. CODEN ASFPDV. ISBN 0-7695-2040-5. ISSN 0272-5428. LCCN QA76 .S979 2003. URL http://ieeexplore.ieee.org/iel5/8767/27770/01238184.pdf?isnumber=27770&prod=CNF&arnumber=1238184&arSt=+92&ared=+101&arAuthor=Kamp%2C+J.

%3B+Zuckerman%2C+D.; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=27770&arnumber=1238184&count=66&index=11. IEEE Computer Society Order Number PR02040.

Kamp:2007:DEB

[KZ07] Jesse Kamp and David Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. *SIAM Journal on Computing*, 36 (5):1231–1247, ???? 2007. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Kumar:2009:UAU

[KZ09] Ajay Kumar and David Zhang. User authentication using fusion of face and palmprint. *International Journal of Image and Graphics (IJIG)*, 9(2):251–270, April 2009. CODEN ???? ISSN 0219-4678.

Ladd:2006:SPS

[Lad06] David Ladd. A software procurement and security primer. *IEEE Security & Privacy*, 4(6):71–73, November/December 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Lafe:2000:CAT

[Laf00] Olu Lafe. *Cellular automata transforms: theory and applications in multimedia compression, encryption and modeling*, volume MMSA16 of *Multimedia systems and applications series*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2000. ISBN 0-7923-7857-1. xii + 177 pp. LCCN QA267.5.C45 L34 2000.

Laih:2003:ACA

[Lai03] Chi Sung Laih, editor. *Advances in Cryptology— ASIACRYPT 2003: 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30–December 4, 2003: Proceedings*, volume 2894 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-20592-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2894.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2894; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b94617.

Laird:2007:THL

[Lai07] Cameron Laird. Taking a hard-line approach to encryption. *Computer*, 40(3): 13–15, March 2007. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Lai:2008:JIA

[Lai08] Charlie Lai. Java insecurity: Accounting for subtleties that can compromise code. *IEEE Software*, 25(1):13–19, January/February 2008. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Lamont:1991:UFC

[Lam91] P. J. C. Lamont. Unique factorization in Cayley arithmetics and cryptology. *Glasgow Mathematical Journal*, 33(3):267–273, ???? 1991. CODEN ???? ISSN 0017-0895 (print), 1469-509X (electronic).

Lam:2001:CCN

[Lam01] Kwok Yan Lam. *Cryptography and computational number theory*, volume 20 of *Progress in computer science and applied logic*. Birkhäuser Verlag, Basel, Switzerland, 2001. ISBN 3-7643-6510-2, 0-8176-6510-2. viii + 378 pp. LCCN QA268 .C77 2001.

Lambert:2007:SLG

[Lam07] David Lambert. *Super little giant book of secret codes*. Sterling Pub. Co., New York, NY, USA, 2007. ISBN 1-4027-3739-4 (paperback). 287 pp. LCCN Z103.3 .L36 2007. URL http://www.loc.gov/catdir/enhancements/fy0738/2007276461-d.html.

Landau:2000:CST

[Lan00a] Susan Landau. Communications security for the Twenty-first Century: The Advanced Encryption Standard. *Notices of the American Mathematical Society*, 47(4):450–459, April 2000. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL http://www.ams.org/notices/200004/fea-landau.pdf.

Landau:2000:STT

[Lan00b] Susan Landau. Standing the test of time: The Data Encryption Standard. *Notices of the American Mathematical Society*, 47(3):341–349, March 2000. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). http://www.ams.org/notices/200003/fea-landau.pdf.

Landau:2000:TOD

[Lan00c] Susan Landau. Technical opinion: designing cryptography for the new century. *Communications of* *the Association for Computing Machinery*, 43(5): 115, May 2000. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/2000-43-5/p115-landau/.

Lanet:2000:ITS

[Lan00d] Jean-Louis Lanet. Invited talk: Are smart cards the ideal domain for applying formal methods? *Lecture Notes in Computer Science*, 1878:363–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1878/18780363.htm; http://link.springer-ny.com/link/service/series/0558/papers/1878/18780363.pdf.

Landau:2004:PNS

[Lan04a] Susan Landau. Polynomials in the nation's service: Using algebra to design the Advanced Encrypted Standard. *American Mathematical Monthly*, 111(2):89–117, February 2004. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). URL http://research.sun.com/people/slandau/maa1.pdf; http://www.esat.kuleuven.ac.be/~rijmen/rijndael; http://www.rsasecurity.com/rsalabs/faq3-1.html.

Landau:2004:SLE

[Lan04b] Susan Landau. Security, liberty, and electronic communications. In Franklin [Fra04], pages 355–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Lakshminarayanan:2008:SUC

[LAPS08] Karthik Lakshminarayanan, Daniel Adkins, Adrian Perrig, and Ion Stoica. Securing user-controlled routing infrastructures. *IEEE/ACM Transactions on Networking*, 16(3):549–561, June 2008. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Laud:2005:STS

[Lau05] Peeter Laud. Secrecy types for a simulatable cryptographic library. In Meadows and Syverson [MS05b], pages 26–35. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Laud:2008:CSC

[Lau08a] Peeter Laud. On the computational soundness of cryptographically masked flows. *ACM SIGPLAN Notices*, 43(1):337–348, January 2008. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Laughlin:2008:CRC

[Lau08b] Robert B. Laughlin. *The crime of reason: and the closing of the scientific mind*. Basic Books, New York, NY, USA, 2008. ISBN 0-465-00507-1. 186 (est.) pp. LCCN JC598 .L38 2008.

Lavington:2006:FCD

[Lav06] Simon Lavington. In the footsteps of Colossus: a description of Oedipus. *IEEE Annals of the History of Computing*, 28(2):44–55, April/June 2006. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic).

Lavoue:2009:LRM

[Lav09] Guillaume Lavoué. A local roughness measure for 3D meshes and its application to visual masking. *ACM Transactions on Applied Perception*, 5(4):21:1–21:??, January 2009. CODEN ???? ISSN 1544-3558 (print), 1544-3965 (electronic).

Lawton:2005:MAH

[Law05] George Lawton. E-mail authentication is here, but has it arrived yet? *Computer*, 38(11):17–19, November 2005. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/comp/mags/co/2005/11/ry017.pdf.

Lawson:2009:SCA

[Law09a] Nate Lawson. Side-channel attacks on cryptographic software. *IEEE Security & Privacy*, 7(6):65–68, November/December 2009. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Lawson:2009:TAG

[Law09b] Nate Lawson. Timing attack in Google Keyczar library. Web site., 2009. URL http://rdist.root.org/2009/05/28/timing-attack-in-google-keyczar-library.

Li:2004:QAU

[LB04] Xiaoyu Li and Howard Barnum. Quantum authentication using entangled states. *International Journal of Foundations of Computer Science (IJFCS)*, 15(4):609–??, August 2004. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Lindskog:2005:DIT

[LB05] Stefan Lindskog and Anna Brunström. Design and implementation of a tunable encryption service for networked applications. Technical report 2005:03, Chalmers tekniska högskola, Göteborg, Sweden, 2005. 17 pp.

Lee:2000:UBN

[LBA00] J. A. N. Lee, C. Burke, and D. Anderson. The US Bombes, NCR, Joseph Desch, and 600 WAVES: the first reunion of the US Naval Computing Machine Laboratory. *IEEE Annals of the History of Computing*, 22(3):27–41, July/September 2000. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL `http://ieeexplore.ieee.org/iel5/85/18655/00859524.pdf`.

Leveiller:2001:CNF

[LBGZ01] Sabine Leveiller, Joseph Boutros, Philippe Guillot, and Gilles Zémor. Cryptanalysis of nonlinear filter generators with $\{0,1\}$-metric Viterbi decoding. *Lecture Notes in Computer Science*, 2260: 402–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600402.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2260/22600402.pdf`.

Leveiller:2002:CNF

[LBGZ02] Sabine Leveiller, Joseph Boutros, Philippe Guillot, and Gilles Zémor. Cryptanalysis of nonlinear filter generators with $\{0,1\}$-metric Viterbi decoding. *Lecture Notes in Computer Science*, 2288: 50–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880050.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2288/22880050.pdf`.

Laufer:2000:SSC

[LBR00] Konstantin Läufer, Gerald Baumgartner, and Vincent F. Russo. Safe structural conformance for Java. *The Computer Journal*, 43 (6):469–481, ???? 2000. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_43/Issue_06/430469.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/`

hdb/Volume_43/Issue_06/pdf/430469.pdf.

Laih:2003:COP

[LC03] C. S. Laih and S. Y. Chiou. Cryptanalysis of an optimized protocol for mobile network authentication and security. *Information Processing Letters*, 85(6): 339–341, March 31, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lin:2004:SOT

[LC04a] Min-Hui Lin and Chin-Chen Chang. A secure one-time password authentication scheme with low-computation for mobile communications. *Operating Systems Review*, 38(2):76–84, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lu:2004:XMS

[LC04b] Eric Jui-Lin Lu and Rai-Fu Chen. An XML multisignature scheme. *Applied Mathematics and Computation*, 149(1):1–14, February 5, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lu:2005:ERU

[LC05a] Rongxing Lu and Zhenfu Cao. Efficient remote user authentication scheme using smart card. *Computer Networks (Amsterdam, Netherlands: 1999)*, 49(4):535–540, November 15, 2005. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Lu:2005:NDA

[LC05b] Rongxing Lu and Zhenfu Cao. A new deniable authentication protocol from bilinear pairings. *Applied Mathematics and Computation*, 168(2):954–961, September 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Long:2005:DTC

[LCC05] Yu Long, Zhenfu Cao, and Kefei Chen. A dynamic threshold commercial key escrow scheme based on conic. *Applied Mathematics and Computation*, 171 (2):972–982, December 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lu:2007:NPL

[LCD07] Rongxing Lu, Zhenfu Cao, and Xiaolei Dong. A new practical limited identity-based encryption scheme. *Fundamenta Informaticae*, 80(4):461–474, December 2007. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Lee:2001:SEK

[LCK01] Byung-Rae Lee, Kyung-Ah Chang, and Tai-Yun Kim. A secure and efficient key escrow protocol for mobile communications. *Lecture Notes in Computer Science*, 2073:433–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2073/20730433.htm; http://link.springer-ny.com/link/service/series/0558/papers/2073/20730433.pdf.

Lee:2003:APS

[LCK03] Jung-Yeun Lee, Jung Hee Cheon, and Seungjoo Kim. An analysis of proxy signatures: Is a secure channel necessary? In Joye [Joy03b], pages 68–79. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Levi:2004:UNC

[LCK04] Albert Levi, M. Ufuk Caglayan, and Cetin K. Koc. Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. *ACM Transactions on Information and System Security*, 7(1):21–59, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2004:DEB

[LCP04] Chang-Doo Lee, Bong-Jun Choi, and Kyoo-Seok Park. Design and evaluation of a block encryption algorithm using dynamic-key mechanism. *Future Generation Computer Systems*, 20(2):327–338, February 16, 2004. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Lim:2009:OPG

[LCS09] Sun Sun Lim, Hichang Cho, and Milagros Rivera Sanchez. Online privacy, government surveillance and national ID cards. *Communications of the Association for Computing Machinery*, 52(12):116–120, December 2009. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Li:2008:CAM

[LCX08] Zhongwen Li, Qiong Chen, and Yang Xiang. A cross-authentication model and implementation. *International Journal of Computer Systems Science and Engi-*

neering, 23(3):??, May 2008. CODEN CSSEEI. ISSN 0267-6192.

Lu:2005:TUS

[LCZ05a] Rong Xing Lu, Zhen Fu Cao, and Yuan Zhou. Threshold undeniable signature scheme based on conic. *Applied Mathematics and Computation*, 162 (1):165–177, March 4, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lu:2005:PBM

[LCZ05b] RongXing Lu, ZhenFu Cao, and Yuan Zhou. Proxy blind multi-signature scheme without a secure channel. *Applied Mathematics and Computation*, 164 (1):179–187, May 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lu:2005:RTP

[LCZ05c] RongXing Lu, ZhenFu Cao, and HaoJin Zhu. A robust $(k, n) + 1$ threshold proxy signature scheme based on factoring. *Applied Mathematics and Computation*, 166(1):35–45, July 6, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Li:2001:CCB

[LD01] Zi Chen Li and Yi Qi Dai. Cryptoanalysis of cryptosystems based on the quadratic residue problem. *J. Tsinghua Univ.*, 41(7):80–82, 2001. CODEN QDXKE8. ISSN 1000-0054.

Lai:2004:SGS

[LD04] Chun-Pong Lai and Cunsheng Ding. Several generalizations of Shamir's secret sharing scheme. *International Journal of Foundations of Computer Science (IJFCS)*, 15(2):445–??, April 2004. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Lavoue:2007:SSW

[LDD07] Guillaume Lavoué, Florence Denis, and Florent Dupont. Subdivision surface watermarking. *Computers and Graphics*, 31(3):480–492, June 2007. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0097849307000507`.

Law:2006:SBB

[LDH06] Yee Wei Law, Jeroen Doumen, and Pieter Hartel. Survey and benchmark of block ciphers for wireless sensor networks. *ACM Transactions on Sensor Networks*, 2(1):65–93, February 2006. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Lindquist:2004:JCS

[LDM04] T. Lindquist, M. Diarra, and B. Millard. A Java cryptography service provider implementing one-time pad (INIDP04). *Proceedings of the Annual Hawaii International Conference on System Sciences*, CONF37:189, 2004. CODEN ???? ISSN 1060-3425.

Lee:2001:AES

[Lee01] Jee Hea Lee. *Authenticated encryption in the symmetric and asymmetric settings*. Vita thesis (Ph.D.), University of California, San Diego, San Diego, CA, USA, 2001.

Lee:2003:BRBa

[Lee03a] Andrew C. Lee. Book review: *Introduction to Cryptography*, by Johannes A. Buchmann. Springer Verlag, 2001. *ACM SIGACT News*, 34(4):15–17, December 2003. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Buc01, Buc04].

Lee:2003:BRBb

[Lee03b] Andrew C. Lee. Book review: *Modern Cryptography, Probabilistic Proofs and Pseudorandomness Algorithms and Combinatorics*, vol 17, by Oded Goldreich. Springer Verlag, 1999. *ACM SIGACT News*, 34(4): 32–34, December 2003. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Gol99].

Lee:2003:CS

[Lee03c] Michael Lee. Cryptanalysis of the SIGABA. Master of Science in Computer Science, Department of Computer Science, University of California, Santa Barbara, Santa Barbara, CA, USA, June 2003. viii + 49 pp. URL `ucsb.curby.net/broadcast/thesis/thesis.pdf`.

Lee:2004:SPM

[Lee04a] Hyang-Sook Lee. A self-pairing map and its applications to cryptography. *Applied Mathematics and Computation*, 151(3):671–678, April 15, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lee:2004:ACA

[Lee04b] Pil Joong Lee, editor. *Advances in cryptology, ASIACRYPT 2004: 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5–9, 2004: Proceedings*, volume 3329 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9.

ISBN 3-540-23975-8 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 2004; QA75.5 .L48 no. 3329. URL http://springerlink.metapress.com/openurl.asp?genre=issue&issn=0302-9743&volume=3329; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b104116.

Lehtinen:2006:CSB

[Leh06] Rick Lehtinen. *Computer Security Basics*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, second edition, 2006. ISBN 0-596-00669-1. 306 (est.) pp. LCCN ???? EUR 38.00.

Lenstra:2001:USM

[Len01] Arjen K. Lenstra. Unbelievable security. matching AES security using public key systems. *Lecture Notes in Computer Science*, 2248:67–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480067.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480067.pdf.

Leroy:2002:BVJ

[Ler02] Xavier Leroy. Bytecode verification on Java smart cards. *Software—Practice and Experience*, 32(4):319–340, April 10, 2002. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic). URL http://www3.interscience.wiley.com/cgi-bin/abstract/91016433/START; http://www3.interscience.wiley.com/cgi-bin/fulltext?ID=91016433&PLACEBO=IE.pdf.

Levy:2001:CHC

[Lev01] Steven Levy. *Crypto: how the code rebels beat the government, saving privacy in the digital age*. Viking, New York, NY, USA, 2001. ISBN 0-670-85950-8, 0-14-024432-8. viii + 356 pp. LCCN QA76.9.A25 L49 2001.

Levy:2002:C

[Lev02] Stephen Levy. *Crypto*. Penguin, London, UK and New York, NY, USA, 2002. ISBN 0-14-024432-8. 368 pp. LCCN ????

Lewand:2000:CM

[Lew00] Robert Edward Lewand. *Cryptological Mathematics*. Mathematical Association of America, Washington, DC, USA, 2000. ISBN 0-88385-719-7. xiv + 1999 pp.

LCCN QA268 .L48 2000. UK£19.95. URL http://www.loc.gov/catdir/description/cam041/00105256.html; http://www.loc.gov/catdir/toc/cam041/00105256.html.

Lee:2003:PKB

[LF03] M. C. Lee and Chun-Kan Fung. A public-key based authentication and key establishment protocol coupled with a client puzzle. *Journal of the American Society for Information Science and Technology: JASIST*, 54(9):810–823, July 2003. CODEN JASIEF. ISSN 1532-2882 (print), 1532-2890 (electronic).

Lei:2007:CSA

[LFHT07] Jun Lei, Xiaoming Fu, Dieter Hogrefe, and Jianrong Tan. Comparative studies on authentication and key exchange methods for 802.11 wireless LAN. *Computers & Security*, 26(5): 401–409, August 2007. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404807000053.

Liaw:2004:SPA

[LFW04] Horng-Twu Liaw, Shiou-Wei Fan, and Wei-Chen Wu. A simple password authentication using a polynomial. *Operating Systems Review*, 38(4):74–79, October 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lekkas:2004:CNL

[LG04] Dimitris Lekkas and Dimitris Gritzalis. Cumulative notarization for long-term preservation of digital signatures. *Computers & Security*, 23(5):413–424, July 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001014.

Levi:2009:ULM

[LG09] Albert Levi and Can Berk Güder. Understanding the limitations of S/MIME digital signatures for e-mails: a GUI based approach. *Computers & Security*, 28(3–4):105–120, May/June 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808000783.

Lan:2010:RNG

[LGKY10] Jingjing Lan, Wang Ling Goh, Zhi Hui Kong, and Kiat Seng Yeo. A random number generator for low power cryptographic application. In *2010 International SoC Design Confer-*

ence (ISOCC)*, pages 328–331. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5682906`.

Lang:2001:CMS

[LGS01] Ulrich Lang, Dieter Gollmann, and Rudolf Schreiner. Cryptography and middleware security. *Lecture Notes in Computer Science*, 2229:408–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290408.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2229/22290408.pdf`.

Lin:2003:PAS

[LH03] Chun-Li Lin and Tzonelih Hwang. A password authentication scheme with secure password updating. *Computers & Security*, 22(1):68–72, January 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404803001147`.

Lee:2004:CUS

[LH04] Narn-Yih Lee and Pei-Hsiu Ho. Convertible undeniable signature with subliminal channels. *Applied Mathematics and Computation*, 158(1):169–175, October 25, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lyda:2007:UEA

[LH07] Robert Lyda and James Hamrock. Using entropy analysis to find encrypted and packed malware. *IEEE Security & Privacy*, 5(2):40–45, March/April 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Li:2008:ISS

[LHC08] Chua-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. Improving the security of a secure anonymous routing protocol with authenticated key exchange for ad hoc networks. *International Journal of Computer Systems Science and Engineering*, 23 (3):??, May 2008. CODEN CSSEEI. ISSN 0267-6192.

Lu:2005:NPS

[LHH05] Eric Jui-Lin Lu, Min-Shiang Hwang, and Cheng-Jian Huang. A new proxy signature scheme with revocation. *Applied Mathematics and Computation*, 161(3):799–806, February 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lee:2002:TDC

[LHL+02] Seonhee Lee, Seokhie Hong, Sangjin Lee, Jongin Lim, and Seonhee Yoon. Truncated differential cryptanalysis of Camellia. *Lecture Notes in Computer Science*, 2288:32–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880032.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880032.pdf`.

Lee:2003:NKA

[LHL03a] Cheng-Chi Lee, Min-Shiang Hwang, and Li-Hua Li. A new key authentication scheme based on discrete logarithms. *Applied Mathematics and Computation*, 139(2–3):343–349, July 15, 2003. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lin:2003:NRU

[LHL03b] Iuon-Chang Lin, Min-Shiang Hwang, and Li-Hua Li. A new remote user authentication scheme for multi-server architecture. *Future Generation Computer Systems*, 19(1): 13–22, January 2003. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Lee:2004:SAA

[LHL04a] Cheng-Chi Lee, Min-Shiang Hwang, and I-En Liao. A server assisted authentication protocol for detecting error vectors. *Operating Systems Review*, 38(2):93–96, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lee:2004:ETP

[LHL04b] Tian-Fu Lee, Tzonelih Hwang, and Chun-Li Lin. Enhanced three-party encrypted key exchange without server public keys. *Computers & Security*, 23(7): 571–577, October 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404804001762`.

Lu:2008:PTZ

[LHL+08] Li Lu, Jinsong Han, Yunhao Liu, Lei Hu, Jin-Peng Huai, Lionel Ni, and Jian Ma. Pseudo trust: Zero-knowledge authentication in anonymous P2Ps. *IEEE Transactions on Parallel and Distributed Systems*, 19(10):1325–1337, October 2008. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Liu:2005:DBV

[LHS05] Hongmei Liu, Jiwu Huang, and Yun Q. Shi. DWT-based video data hiding robust to MPEG compression and frame loss. *International Journal of Image and Graphics (IJIG)*, 5(1):111–??, January 2005. CODEN ???? ISSN 0219-4678.

Lee:2009:NCA

[LHT09] Cheng-Chi Lee, Min-Shiang Hwang, and Shiang-Feng Tzeng. A new convertible authenticated encryption scheme based on the ElGamal cryptosystem. *International Journal of Foundations of Computer Science (IJFCS)*, 20(2):351–359, April 2009. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Lee:2002:FRU

[LHY02] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Peng Yang. A flexible remote user authentication scheme using Smart Cards. *Operating Systems Review*, 36(3):46–52, July 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lee:2005:NBS

[LHY05] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. A new blind signature based on the discrete logarithm problem for untraceability. *Applied Mathematics and Computation*, 164 (3):837–841, May 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Li:2001:NSA

[Li01] Yifa Li. A new semantics of authentication logic. *Lecture Notes in Computer Science*, 2229:476–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290476.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290476.pdf`.

Li:2005:ABPa

[Li05] S. Z. Li, editor. *Advances in biometric person authentication: 5th Chinese conference on biometric recognition, SINOBIOMETRICS 2004, Guangzhou, China, December 13–14, 2004, proceedings*, volume 3338 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-24029-2 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.B56 C4 2004. URL `http://www.springerlink.com/openurl.asp?genre=issue&`

issn=0302-9743&volume=3338.

Lieman:2005:CRW

[Lie05] Daniel Lieman. Cryptography in the real world today. In Garrett and Lieman [GL05], pages 63–72. ISBN 0-8218-3365-0. LCCN QA76.9.A25 P82 2005. URL http://www.loc.gov/catdir/toc/fy0612/2005048178.html.

Lin:2000:RTI

[Lin00a] Phen-Lan Lin. Robust transparent image watermarking system with spatial mechanisms. *The Journal of Systems and Software*, 50(2):107–116, February 15, 2000. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.elsevier.nl/gej-ng/10/29/11/49/27/27/article.pdf; http://www.elsevier.nl/gej-ng/10/29/11/49/27/abstract.html.

Linn:2000:TMM

[Lin00b] John Linn. Trust models and management in public-key infrastructures. Technical report, RSA Data Security, Inc., Redwood City, CA, USA, November 6, 2000. 13 pp. URL ftp://ftp.rsasecurity.com/pub/pdfs/PKIPaper.pdf.

Lin:2001:HKA

[Lin01a] Chu-Hsing Lin. Hierarchical key assignment without public-key cryptography. *Computers & Security*, 20(7):612–619, October 31, 2001. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404801007118.

Lin:2001:DWM

[Lin01b] Phen-Lan Lin. Digital watermarking models for resolving rightful ownership and authenticating legitimate customer. *The Journal of Systems and Software*, 55(3):261–271, January 15, 2001. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.elsevier.nl/gej-ng/10/29/11/54/27/27/abstract.html; http://www.elsevier.nl/gej-ng/10/29/11/54/27/27/article.pdf.

Lindell:2001:PCT

[Lin01c] Yehuda Lindell. Parallel coin-tossing and constant-round secure two-party computation. In Kilian [Kil01a], pages 171–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/

bibs/2139/21390171.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390171.pdf.

Lingmann:2002:DSK

[Lin02] Thomas Lingmann. *Datenverschlüsselung: sichere Kommunikation mit Linux und BSD: Security mit Open Source. (German) [Data encoding: Secure communication with Linux and BSD: Security with Open Source].* C & L, Böblingen, Germany, 2002. ISBN 3-932311-87-8 (??invalid checksum??). 476 (est.) pp. LCCN ????

Lindell:2003:SCC

[Lin03] Yehuda Lindell. A simpler construction of CCA2-secure public-key encryption under general assumptions. *Lecture Notes in Computer Science*, 2656: 241–254, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_15.pdf.

Lin:2007:PFT

[Lin07] Jenn-Wei Lin. Providing fault-tolerant authentication and authorization in wireless mobile IP networks. *The Journal of Systems and Software*, 80 (2):149–163, February 2007. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Lee:2005:IEC

[LJ05a] B. K. Lee and L. K. John. Implications of executing compression and encryption applications on general purpose processors. *IEEE Transactions on Computers*, 54(7):917–922, July 2005. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1432674.

Licks:2005:GAI

[LJ05b] Vinicius Licks and Ramiro Jordan. Geometric attacks on image watermarking systems. *IEEE MultiMedia*, 12 (3):68–78, July/September 2005. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Li:2005:AWP

[LJL05] Zhitang Li, Huijun Jiang, and Hanju Li. Active worm propagation model with discrete time. In Han et al. [HYZ05b], pages 122–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Lee:2004:SSP

[LJY04] Jung-Seuk Lee, Jun-Cheol Jeon, and Kee-Young Yoo.

A security scheme for protecting security policies in firewall. *Operating Systems Review*, 38(2):69–72, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Ludwig:2001:FSE

[LK01] Stefan Ludwig and Winfried Kalfa. File system encryption with integrated user management. *Operating Systems Review*, 35(4):88–93, October 2001. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lee:2008:SAF

[LKH+08] Changhoon Lee, Jongsung Kim, Seokhie Hong, Jaechul Sung, and Sangjin Lee. Security analysis of the full-round DDO-64 block cipher. *The Journal of Systems and Software*, 81(12):2328–2335, December 2008. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Lee:2009:SAF

[LKHL09] C. Lee, J. Kim, S. Hong, and Y.-S. Lee. Security analysis of the full-round CHESS-64 cipher suitable for pervasive computing environments. *J.UCS: Journal of Universal Computer Science*, 15(5):1007–??, ???? 2009. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_15_5/security_analysis_of_the.

Lim:2001:SAW

[LKJL01] Shin-Young Lim, Jeong-Ho Ko, Eun-Ah Jun, and Gang-Soo Lee. Specification and analysis of n-way key recovery system by Extended Cryptographic Timed Petri Net. *The Journal of Systems and Software*, 58(2):93–106, September 1, 2001. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.elsevier.com/gej-ng/10/29/11/68/33/28/abstract.html.

Lee:2003:PSAa

[LKKY03a] Sung-Woon Lee, Woo-Hun Kim, Hyun-Sung Kim, and Kee-Young Yoo. Parallizable simple authenticated key agreement protocol. *Operating Systems Review*, 37(2):13–18, April 2003. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lee:2003:PSAb

[LKKY03b] Sung-Woon Lee, Woo-Hun Kim, Hyun-Sung Kim, and Kee-Young Yoo. Parallizable simple authenticated key agreement protocol. *Operating Systems Review*, 37(3):17–22, July 2003. CODEN OSRED8. ISSN 0163-

5980 (print), 1943-586X (electronic).

Lee:2005:NIW

[LKLK05] Joong-Jae Lee, Won Kim, Na-Young Lee, and Gye-Young Kim. A new incremental watermarking based on dual-tree complex wavelet transform. *The Journal of Supercomputing*, 33(1):133–140, July 2005. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=33&issue=1&spage=133.

Lee:2005:APC

[LKM+05] Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, and Zhenghong Wang. Architecture for protecting critical secrets in microprocessors. *ACM SIGARCH Computer Architecture News*, 33(2):2–13, May 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Lee:2004:CUA

[LKY04] Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo. Cryptanalysis of a user authentication scheme using hash functions. *Operating Systems Review*, 38(1):24–28, January 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lee:2005:ENB

[LKY05a] Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo. Efficient nonce-based remote user authentication scheme using smart cards. *Applied Mathematics and Computation*, 167(1):355–361, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lee:2005:EVB

[LKY05b] Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo. Efficient verifier-based key agreement protocol for three parties without server's public key. *Applied Mathematics and Computation*, 167(2):996–1003, August 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lee:2005:IHA

[LKY05c] Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo. Improvement of HWWM-authenticated key agreement protocol. *Applied Mathematics and Computation*, 162(3):1315–1320, March 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lee:2005:ILL

[LKY05d] Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo. Improvement of Lee and Lee's authenticated key agreement scheme. *Applied Mathematics and Computation*, 162(3):1049–1053, March 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lim:2000:GTC

[LKYL00] Seongan Lim, Seungjoo Kim, Ikkwon Yie, and Hongsub Lee. A generalized Takagi-cryptosystem with a modulus of the form $p^r q^s$. *Lecture Notes in Computer Science*, 1977: 283–294, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Luo:2004:UUR

[LKZ+04] Haiyun Luo, Jiejun Kong, Petros Zerfos, Songwu Lu, and Lixia Zhang. URSA: ubiquitous and robust access control for mobile ad hoc networks. *IEEE/ACM Transactions on Networking*, 12(6):1049–1063, December 2004. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Lu:2001:DWC

[LL01] Chun-Shien Lu and Hong-Yuan Mark Liao. Digital watermarking: a communications with side information perspective. *Lecture Notes in Computer Science*, 2195:927–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950927.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950927.pdf.

Lou:2002:SMS

[LL02] Der-Chyuan Lou and Jiang-Lung Liu. Steganographic method for secure communications. *Computers & Security*, 21(5):449–460, October 1, 2002. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404802005151.

Lee:2003:ISC

[LL03] Pil Joong Lee and Chae Hoon Lim, editors. *Information security and cryptology — ICISC 2002: 5th International Conference, Seoul, Korea, November 28–29, 2002: Revised Papers*, volume 2587 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CO-

DEN LNCSD9. ISBN 3-540-00716-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I32 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2587.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2587. Also available via the World Wide Web.

Lee:2004:FIM

[LL04a] Narn-Yih Lee and Ming-Feng Lee. Further improvement on the modified authenticated key agreement scheme. *Applied Mathematics and Computation*, 157(3):729–733, October 15, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lee:2004:CIB

[LL04b] Wei-Bin Lee and Kuan-Chieh Liao. Constructing identity-based cryptosystems for discrete logarithm based cryptosystems. *Journal of Network and Computer Applications*, 27(4):191–199, November 2004. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804504000268.

Lee:2004:DIS

[LL04c] Wongoo Lee and Jaekwang Lee. Design and implementation of secure e-mail system using elliptic curve cryptosystem. *Future Generation Computer Systems*, 20(2):315–326, February 16, 2004. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Lim:2004:ISC

[LL04d] Jong In Lim and Dong Hoon Lee, editors. *Information Security and Cryptology—ICISC 2003: 6th International Conference, Seoul, Korea, November 27–28, 2003: Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-21376-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://link.springer-ny.com/link/service/series/0558/tocs/t2971.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2971; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b96249.

Lee:2005:CMA

[LL05a] Keon-Jik Lee and Byeong-Jik Lee. Cryptanalysis of the modified authenticated key agreement scheme. *Applied Mathematics and Computation*, 170 (1):280–284, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lee:2005:SSP

[LL05b] Narn-Yih Lee and Ming-Feng Lee. The security of a strong proxy signature scheme with proxy signer privacy protection. *Applied Mathematics and Computation*, 161(3):807–812, February 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Li:2005:FCR

[LL05c] Ying Li and Jintao Li. Further cryptanalysis of a remote login authentication scheme based on geometric approach. In Han et al. [HYZ05b], pages 143–?? ISBN 981-270-153-2. LCCN ???? URL `http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html`.

Lee:2006:ISC

[LL06] Wei-Bin Lee and Kuan-Chieh Liao. Improved self-certified group-oriented cryptosystem without a combiner. *The Journal of Systems and Software*, 79(4):502–506, April 2006. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Lu:2006:FBW

[LLC06a] Wei Lu, Hongtao Lu, and Fu-Lai Chung. Feature based watermarking using watermark template match. *Applied Mathematics and Computation*, 177(1):377–386, June 1, 2006. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lu:2006:RDI

[LLC06b] Wei Lu, Hongtao Lu, and Fu-Lai Chung. Robust digital image watermarking based on subsampling. *Applied Mathematics and Computation*, 181(2):886–893, October 15, 2006. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Li:2008:CRR

[LLCL08] Shujun Li, Chengqing Li, Guanrong Chen, and Kwok-Tung Lo. Cryptanalysis of the RCES/RSES image encryption scheme. *The Journal of Systems and Software*, 81(7):1130–1143, July 2008. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Lee:2001:PBG

[LLH01] Eonkyung Lee, Sang Jin Lee, and Sang Geun Hahn. Pseudorandomness from braid groups. In Kilian [Kil01a], pages 486–

?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390486.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390486.pdf.

Lee:2002:RUA

[LLH02] Cheng-Chi Lee, Li-Hua Li, and Min-Shiang Hwang. A remote user authentication scheme using hash functions. *Operating Systems Review*, 36(4):23–29, October 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Li:2004:CES

[LLH04] Li-Hua Li, Chi-Yu Liu, and Min-Shiang Hwang. Cryptanalysis of an efficient secure group signature scheme. *Operating Systems Review*, 38 (4):66–69, October 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Liao:2006:PAS

[LLH06] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang. A password authentication scheme over insecure networks. *Journal of Computer and System Sciences*, 72(4): 727–740, June 2006. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000005001157.

Lesniewski-Laas:2005:SSS

[LLK05] Chris Lesniewski-Laas and M. Frans Kaashoek. SSL splitting: Securely serving data from untrusted caches. *Computer Networks (Amsterdam, Netherlands: 1999)*, 48(5):763–779, August 5, 2005. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Li:2001:SPD

[LLL+01] Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou, and Yuanlong Cai. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. *Lecture Notes in Computer Science*, 2260:205–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600205.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600205.pdf.

Lee:2002:SEC

[LLL02] Hyung-Woo Lee, Sung-

Min Lee, and Im-Yeong Lee. Secure electronic copyright distribution with public key based traitor tracing. *Lecture Notes in Computer Science*, 2455: 324–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2455/24550324.htm; http://link.springer-ny.com/link/service/series/0558/papers/2455/24550324.pdf.

Lee:2004:MPA

[LLL04] Young-Ran Lee, Hyang-Sook Lee, and Ho-Kyu Lee. Multi-party authenticated key agreement protocols from multi-linear forms. *Applied Mathematics and Computation*, 159(2):317–331, December 6, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Li:2006:ESY

[LLLZ06a] Chengqing Li, Shujun Li, Der-Chyuan Lou, and Dan Zhang. Erratum to "On the security of the Yen-Guo's domino signal encryption algorithm (DSEA)" [The Journal of Systems and Software 79 (2006) 253–258]. *The Journal of Systems and Software*, 79(12):1789, December 2006. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). See [LLLZ06b].

Li:2006:SYG

[LLLZ06b] Chengqing Li, Shujun Li, Der-Chyuan Lou, and Dan Zhang. On the security of the Yen–Guo's domino signal encryption algorithm (DSEA). *The Journal of Systems and Software*, 79 (2):253–258, February 2006. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). See erratum [LLLZ06a].

LaMacchia:2007:SSA

[LLM07] Brian LaMacchia, Kristin Lauter, and Anton Mityagin. Stronger security of authenticated key exchange. In Willy Susilo, Joseph K. Liu, and Yi Mu, editors, *Provable Security First International Conference, ProvSec 2007, Wollongong, Australia, November 1–2, 2007. Proceedings*, pages 1–16. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. URL https://link.springer.com/chapter/10.1007/978-3-540-75670-5_1.

Lindell:2002:CAB

[LLR02] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. On the composition of authenticated Byzantine agreement.

In ACM [ACM02], pages 514–523. ISBN 1-58113-495-9. LCCN QA75.5 .A22 2002. ACM order number 508020.

Lindell:2006:CAB

[LLR06] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. On the composition of authenticated Byzantine Agreement. *Journal of the ACM*, 53(6): 881–917, November 2006. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Lian:2007:MDE

[LLRW07] S. Lian, Z. Liu, Z. Ren, and Z. Wang. Multimedia data encryption in block-based codecs. *International Journal of Computer Applications*, 29(1): 18–24, 2007. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2007.11441828`.

Lee:2005:IWR

[LLS05a] Choong-Hoon Lee, Heung-Kyu Lee, and Youngho Suh. Image watermarking resistant to combined geometric and removal attacks. *International Journal of Image and Graphics (IJIG)*, 5(1): 37–??, January 2005. CODEN ???? ISSN 0219-4678.

Liu:2005:SWA

[LLS05b] Sanya Liu, Zhenyu Liu, and Zhongren Su. Securing Web application system: a solution based on SMS for identifying users. In Han et al. [HYZ05b], pages 104–?? ISBN 981-270-153-2. LCCN ???? URL `http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html`.

Lee:2009:CET

[LLS+09] Tian-Fu Lee, Jenn-Long Liu, Mei-Jiun Sung, Shiueng-Bien Yang, and Chia-Mei Chen. Communication-efficient three-party protocols for authentication and key agreement. *Computers and Mathematics with Applications*, 58(4):641–648, August 2009. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122109003757`.

Li:2004:ABP

[LLT+04] Stan Z. Li, Jianhuang Lai, Tieniu Tan, Guocan Feng, and Yunhong Wang, editors. *Advances in Biometric Person Authentication: 5th Chinese Conference on Biometric Recognition, SINOBIOMETRICS 2004, Guangzhou, China, December 13–14, 2004: Proceedings*, volume 3338 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CO-

DEN LNCSD9. ISBN 3-540-24029-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.B56 C4 2004. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3338; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b104239.

Li:2005:ATN

[LLW05] Jiangtao Li, Ninghui Li, and William H. Winsborough. Automated trust negotiation using cryptographic credentials. In Meadows and Syverson [MS05b], pages 46–57. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Liu:2008:DEA

[LLW08a] Hongjun Liu, Ping Luo, and Daoshun Wang. A distributed expansible authentication model based on Kerberos. *Journal of Network and Computer Applications*, 31(4):472–486, November 2008. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804508000027.

Liu:2008:SAM

[LLW08b] Hongjun Liu, Ping Luo, and Daoshun Wang. A scalable authentication model based on public keys. *Journal of Network and Computer Applications*, 31(4):375–386, November 2008. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804508000106.

Li:2009:ATN

[LLW09] Jiangtao Li, Ninghui Li, and William H. Winsborough. Automated trust negotiation using cryptographic credentials. *ACM Transactions on Information and System Security*, 13(1):2:1–2:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2006:DCK

[LLY06] Patrick P. C. Lee, John C. S. Lui, and David K. Y. Yau. Distributed collaborative key agreement and authentication protocols for dynamic peer groups. *IEEE/ACM Transactions on Networking*, 14(2):263–276, April 2006. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Linares:2000:SAM

[LM00] Leandro Rodríguez Liñares and Carmen García Mateo. A speaker authentication module in TelCorreo. *Lecture Notes in Computer Science*, 1902:375–??, 2000. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1902/19020375.htm; http://link.springer-ny.com/link/service/series/0558/papers/1902/19020375.pdf.

Lorenz:2002:SSG

[LM02] U. Lorenz and B. Monien. The secret of selective game tree search, when using random-error evaluations. *Lecture Notes in Computer Science*, 2285: 203–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2285/22850203.htm; http://link.springer-ny.com/link/service/series/0558/papers/2285/22850203.pdf.

Lavasani:2008:IFA

[LM08] Ahmad Lavasani and Reza Mohammadi. Implementing a feasible attack against ECC2K-130 certicom challenge (abstract only). *ACM Communications in Computer Algebra*, 42(1–2):61–62, March/June 2008. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Li:2003:SCE

[LMC+03] Shujun Li, Xuanqin Mou, Yuanlong Cai, Zhen Ji, and Jihong Zhang. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. *Computer Physics Communications*, 153(1):52–58, June 1, 2003. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465502008755.

Lamenca-Martinez:2006:LNP

[LMHCETR06] Carlos Lamenca-Martinez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. Lamar: a new pseudorandom number generator evolved by means of genetic programming. *Lecture Notes in Computer Science*, 4193:850–859, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/c60q42qt2m035685/.

Leitold:2001:MTN

[LMP+01] Herbert Leitold, Wolfgang Mayerwieser, Udo Payer, Karl Christian Posch, Reinhard Posch, and Johannes Wolkerstorfer. A 155 Mbps Triple-DES network encryptor. *Lecture Notes in*

Computer Science, 1965: 164–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650164.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650164.pdf.

Lepinski:2005:FZK

[LMS05] Matt Lepinski, Silvio Micali, and Abhi Shelat. Fair-zero knowledge. In Kilian [Kil05], pages 245–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Laskari:2007:AEC

[LMSV07] E. C. Laskari, G. C. Meletiou, Y. C. Stamatiou, and M. N. Vrahatis. Applying evolutionary computation methods for the cryptanalysis of Feistel ciphers. *Applied Mathematics and Computation*, 184(1):63–72, January 1, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Laskari:2005:TTC

[LMTV05] E. C. Laskari, G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis. Transformations of two cryptographic problems in terms of matrices. *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 39(4):127–130, December 2005. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

Lu:2005:CCA

[LMV05] Yi Lu, Willi Meier, and Serge Vaudenay. The conditional correlation attack: a practical attack on Bluetooth encryption. In Shoup [Sho05a], pages 97–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Li:2005:BPC

[LMW05] Ninghui Li, John C. Mitchell, and William H. Winsborough. Beyond proof-ofcompliance: security analysis in trust management. *Journal of the ACM*, 52(3): 474–514, May 2005. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Liu:2004:MBA

[LN04] Donggang Liu and Peng Ning. Multilevel μTESLA: Broadcast authentication for distributed sensor networks. *ACM Transactions on Embedded Computing Systems*, 3(4):800–836, November 2004. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Levieil:2008:CTC

[LN08] Eric Levieil and David Naccache. Cryptographic test correction. *IEEE Security & Privacy*, 6(2):69–71, March/April 2008. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Liu:2008:ARL

[LNL+08] Donggang Liu, Peng Ning, An Liu, Cliff Wang, and Wenliang Kevin Du. Attack-resistant location estimation in wireless sensor networks. *ACM Transactions on Information and System Security*, 11(4):22:1–22:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lotspiech:2002:CFB

[LNP02] Jeffrey Lotspiech, Stefan Nusser, and Florian Pestoni. Cover feature: Broadcast encryption's bright future. *Computer*, 35(8):57–63, August 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://csdl.computer.org/dl/mags/co/2002/08/r8057.htm`; `http://csdl.computer.org/dl/mags/co/2002/08/r8057.pdf`; `http://www.computer.org/computer/co2002/r8057abs.htm`.

Li:2002:HNP

[LNS02] Wen-Ching W. Li, Mats Näslund, and Igor E. Shparlinski. Hidden number problem with the trace and bit security of XTR and LUC. In Yung [Yun02a], pages 433–448. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442`.

Loidreau:2000:SMC

[Loi00] Pierre Loidreau. Strengthening McEliece cryptosystem. *Lecture Notes in Computer Science*, 1976: 585–598, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lopez:2004:AAI

[LOP04] Javier Lopez, Rolf Oppliger, and Günther Pernul. Authentication and authorization infrastructures (AAIs): a comparative survey. *Computers & Security*, 23(7): 578–590, October 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404804001828`.

Lopez:2006:UPK

[Lop06] Javier Lopez. Unleashing public-key cryptography in wireless sensor networks. *Journal of Computer Security*, 14(5):469–482, ???? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lovering:2001:TKF

[Lov01] Daniel Lovering. Taming the killing fields of Laos: Live bombs from the Vietnam War continue to kill people and hamper agricultural development in Laos. the cleanup project required deciphering decadesold computer files. *Scientific American*, 285(2):66–71, August 2001. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.sciam.com/2001/0801issue/2001/0801issue/0801hargrove.html`.

Lindell:2000:PPD

[LP00] Yehuda Lindell and Benny Pinkas. Privacy preserving data mining. In Bellare [Bel00], pages 36–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800036.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1880/18800036.pdf`.

Lysyanskaya:2001:AST

[LP01] Anna Lysyanskaya and Chris Peikert. Adaptive security in the threshold setting: From cryptosystems to signature schemes. *Lecture Notes in Computer Science*, 2248:331–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480331.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2248/22480331.pdf`.

Labbe:2002:AIF

[LP02a] Anna Labbé and Annie Pérez. AES implementation on FPGA: Time — flexibility tradeoff. *Lecture Notes in Computer Science*, 2438:836–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2438/24380836.htm; http://link.springer-ny.com/link/service/series/0558/papers/2438/24380836.pdf`.

Luccio:2002:AC

[LP02b] Fabrizio Luccio and Linda Pagli. From algorithms to cryptography. *Lecture Notes in Computer Science*, 2286:15–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2286/22860015.htm; http://link.springer-ny.com/link/service/series/0558/papers/2286/22860015.pdf`.

Lee:2003:CPK

[LP03] Eonkyung Lee and Je Hong Park. Cryptanalysis of the public-key encryption based on braid groups. *Lecture Notes in Computer Science*, 2656:477–490, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/3-540-39200-9_30.pdf`.

Li:2005:MCK

[LPM05] Mingyan Li, Radha Poovendran, and David A. McGrew. Minimizing center key storage in hybrid one-way function based group key management with communication constraints. *Information Processing Letters*, 93(4):191–198, February 28, 2005. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Law:2009:EEL

[LPV+09] Yee Wei Law, Marimuthu Palaniswami, Lodewijk Van Hoesel, Jeroen Doumen, Pieter Hartel, and Paul Havinga. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. *ACM Transactions on Sensor Networks*, 5(1):6:1–6:??, February 2009. CODEN ????. ISSN 1550-4859 (print), 1550-4867 (electronic).

Lemke:2006:ESC

[LPW06] Kerstin Lemke, Christof Paar, and Marko Wolf, editors. *Embedded security in cars: securing current and* *future automotive IT applications*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-540-28384-6. x + 273 pp. LCCN TL275.E53 2006.

Li:2006:PMW

[LPZ06] Li Li, Zhigeng Pan, and David Zhang. A public mesh watermarking algorithm based on addition property of Fourier Transform. *International Journal of Image and Graphics (IJIG)*, 6(1):35–??, January 2006. CODEN ???? ISSN 0219-4678.

Li:2008:DEO

[LQ08] Lvzhou Li and Daowen Qiu. Determining the equivalence for one-way quantum finite automata. *Theoretical Computer Science*, 403(1):42–51, August 20, 2008. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Lientz:2001:BTP

[LR01] Bennet P. Lientz and Kathryn P. Rea. *Breakthrough technology project management*. Academic Press, New York, NY, USA, 2001. ISBN 0-12-449968-6. xxv + 342 pp. LCCN HD69.P75 L538 2001. US$44.95.

Lemke-Rust:2007:MAP

[LR07] Kerstin Lemke-Rust. *Models and Algorithms for Physical Cryptanalysis*, volume 4 of *IT-Security*. Europäischer Universitätsverlag, Bochum, Germany, 2007. ISBN 3-89966-272-5. ISSN 1864-1709. xiv + 232 pp. LCCN ???? EUR 24.90.

Liskov:2002:TBC

[LRW02] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In Yung [Yun02a], pages 31–46. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL `http://link.springer.de/link/service/series/0558/bibs/2442/24420031.htm`; `http://link.springer.de/link/service/series/0558/papers/2442/24420031.pdf`.

Lenstra:2001:SFR

[LS01a] Arjen K. Lenstra and Igor E. Shparlinski. Selective forgery of RSA signatures with fixed-pattern padding. *Lecture Notes in Computer Science*, 2274:228–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740228.htm`;

http://link.springer-ny.com/link/service/series/0558/papers/2274/22740228.pdf.

Lindemann:2001:ICT

[LS01b] Mark Lindemann and Sean W. Smith. Improving DES coprocessor throughput for short operations. In USENIX [USE01c], page ?? ISBN 1-880446-18-9, 1-880446-07-3. LCCN QA76.9.A25 U565 2001. URL http://www.usenix.org/publications/library/proceedings/sec01/lindemann.html.

Loidreau:2001:WKM

[LS01c] Pierre Loidreau and Nicolas Sendrier. Weak keys in the McEliece public-key cryptosystem. *IEEE Transactions on Information Theory*, 47(3):1207–1211, March 2001. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Li:2005:ULC

[LS05a] Chung-Chih Li and Bo Sun. Using linear congruential generators for cryptographic purposes. In Gongzhu Hu, editor, *Computers and their applications: proceedings of the ISCA 20th international conference ; New Orleans, Louisiana, USA, March 16–18, 2005*, pages 13–19. International Society for Computers and Their Applications, Cary, NC, USA, 2005. ISBN 1-880843-54-4. LCCN QA76.76.A65 I83 2005.

Liang:2005:FAG

[LS05b] Zhenkai Liang and R. Sekar. Fast and automated generation of attack signatures: a basis for building self-protecting servers. In Meadows and Syverson [MS05b], pages 213–222. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Liu:2008:GPV

[LS08] Jen-Chang Liu and Ming-Hong Shih. Generalizations of pixel-value differencing steganography for data hiding in images. *Fundamenta Informaticae*, 83 (3):319–335, August 2008. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Lopez:2007:SCB

[LSA+07] Andrés Marín López, Daniel Díaz Sánchez, Florina Almenárez, Carlos García Rubio, and Celeste Campo. Smart card-based agents for fair non-repudiation. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(9):2288–2298, June 20, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Lin:2003:DBI

[LSC03] S. D. Lin, S. C. Shie, and C. F. Chen. A DCT-based image watermarking with threshold embedding. *International Journal of Computer Applications*, 25(2): 130–135, 2003. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.1080/1206212X.2003.11441694.

Lin:2000:TPE

[LSH00] Chun-Li Lin, Hung-Min Sun, and Tzonelih Hwang. Three-party encrypted key exchange: attacks and a solution. *Operating Systems Review*, 34(4):12–20, October 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lin:2003:SEOa

[LSH03a] Chih-Wei Lin, Jau-Ji Shen, and Min-Shiang Hwang. Security enhancement for Optimal Strong-Password Authentication protocol. *Operating Systems Review*, 37 (2):7–12, April 2003. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lin:2003:SEOb

[LSH03b] Chih-Wei Lin, Jau-Ji Shen, and Min-Shiang Hwang. Security enhancement for Optimal Strong-Password Authentication Protocol. *Operating Systems Review*, 37 (3):12–16, July 2003. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lu:2005:BIW

[LSKC05] Haiping Lu, Yun Q. Shi, Alex C. Kot, and Lihui Chen. Binary image watermarking through blurring and biased binarization. *International Journal of Image and Graphics (IJIG)*, 5(1):67–??, January 2005. CODEN ???? ISSN 0219-4678.

Li:2005:ABPb

[LST+05] Stan Z. Li, Zhenan Sun, Tieniu Tan, Sharath Pankanti, Gérard Chollet, and David Zhang, editors. *Advances in biometric person authentication: International Workshop on Biometric Recognition Systems, IWBRS 2005, Beijing, China, October 22–23, 2005: proceedings*, volume 3781 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-29431-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.B56 I58 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3781.

Liang:2009:AIE

[LSVS09] Zhenkai Liang, Weiqing Sun, V. N. Venkatakrishnan, and R. Sekar. Alcatraz: An isolated environment for experimenting with untrusted software. *ACM Transactions on Information and System Security*, 12(3):14:1–14:37, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2001:EPI

[LSY01] Ruby B. Lee, Zhijie Shi, and Xiao Yang. Efficient permutation instructions for fast software cryptography. *IEEE Micro*, 21(6):56–69, November/ December 2001. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL `http://dlib.computer.org/mi/books/mi2001/m6056abs.htm; http://dlib.computer.org/mi/books/mi2001/pdf/m6056.pdf`.

Liu:2005:RBU

[LSZ05] Linlan Liu, Jian Shu, and Jianxiang Zheng. The RBAC-based user authorization in Sanxin ERP system. In Han et al. [HYZ05b], pages 155–?? ISBN 981-270-153-2. LCCN ???? URL `http://eproceedings.worldscinet.com/9812701532/9812701532_0031.html`.

Lin:2004:SIS

[LT04] Chang-Chou Lin and Wen-Hsiang Tsai. Secret image sharing with steganography and authentication. *The Journal of Systems and Software*, 73(3):405–414, November/December 2004. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Li:2005:ISS

[LTH05] Li-Hua Li, Shiang-Feng Tzeng, and Min-Shiang Hwang. Improvement of signature scheme based on factoring and discrete logarithms. *Applied Mathematics and Computation*, 161 (1):49–54, February 4, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lie:2000:ASC

[LTM+00] David Lie, Chandramohan Thekkath, Mark Mitchell, Patrick Lincoln, Dan Boneh, John Mitchell, and Mark Horowitz. Architectural support for copy and tamper resistant software. *ACM SIGPLAN Notices*, 35(11): 168–177, November 2000. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Lin:2005:HAO

[LTW05] Henry Lin, Luca Trevisan, and Hoeteck Wee. On hardness amplification of one-way functions. In Kilian [Kil05], pages 34–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Lu:2002:HEA

[Lu02] Chi-Jen Lu. Hyper-encryption against space-bounded adversaries from on-line strong extractors. In Yung [Yun02a], pages 257–271. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420257.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420257.pdf.

Lu:2007:NSC

[Lu07] HongQian Karen Lu. Network smart card review and analysis. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(9):2234–2248, June 20, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Lucks:2000:ASR

[Luc00] Stefan Lucks. Attacking seven rounds of Rijndael under 192-bit and 256-bit keys. In NIST [NIS00], pages 215–229. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Lucks:2002:SAB

[Luc02a] Stefan Lucks. The saturation attack — A bait for Twofish. *Lecture Notes in Computer Science*, 2355:1–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550001.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550001.pdf.

Lucks:2002:VCS

[Luc02b] Stefan Lucks. A variant of the Cramer–Shoup cryptosystem for groups of unknown order. *Lecture Notes in Computer Science*, 2501:27–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2501/25010027.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010027.pdf`.

Lucas:2006:PGE

[Luc06] Michael Lucas. *PGP and GPG: email for the practical paranoid*. No Starch Press, San Francisco, CA, USA, 2006. ISBN 1-59327-071-2. 216 (est.) pp. LCCN TK5102.85 .L83 2006. URL `http://www.loc.gov/catdir/toc/ecip061/2005028824.html; http://www.nostarch.com/pgp.htm`.

Ludvig:2005:PWF

[Lud05] Michal Ludvig. VIA PadLock-wicked fast encryption. *Linux Journal*, 2005(133):4, May 2005. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Lukyanov:2001:PFA

[Luk01] Dmitro O. Luk'yanov. On the problem of the formation of an authentication protocol for on-line cryptosystems. *Vīsn. Kiï v. Unīv. Ser. Fīz.-Mat. Nauki*, 2:269–276, 2001.

Lunde:2009:BCU

[Lun09] Paul Lunde, editor. *The book of codes: understanding the world of hidden messages: an illustrated guide to signs, symbols, ciphers, and secret languages*. University of California Press, Berkeley, CA, 2009. ISBN 0-520-26013-9. 279 pp. LCCN Z103 .B56 2009. URL `http://www.loc.gov/catdir/enhancements/fy1002/2009281679-b.html; http://www.loc.gov/catdir/enhancements/fy1002/2009281679-d.html`.

Lutz:2002:BBS

[Lut02] Michael J. Lutz. Bookshelf: Balancing speed and complexity with compilers; advanced cryptology text; computer architecture basics; mutation testing compendium. *Computer*, 35(4):89, April 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co2002/pdf/r4089.pdf; http://www.computer.org/computer/co2002/r4089abs.htm`.

Lutz:2003:BLF

[Lut03] Michael J. Lutz. Bookshelf: Laying the foundation for pervasive computing [Pervasive Computing]; integrated approach to data handling [Exploratory Data Mining and Data Cleaning]; making theory practical [Modern Cryptography: Theory and Practice]; detailed look at systems testing [Testing of Digital Systems]. *Computer*, 36(10): 102, October 2003. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/dl/mags/co/2003/10/rx102.htm; http://www.computer.org/computer/co2003/rx102.pdf.

Lenstra:2000:XPK

[LV00] Arjen K. Lenstra and Eric R. Verheul. The XTR public key system. In Bellare [Bel00], pages 1–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800001.pdf.

Lu:2004:FCA

[LV04] Yi Lu and Serge Vaudenay. Faster correlation attack on Bluetooth keystream generator E0. In Franklin [Fra04], pages 407–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Laguillaumie:2007:MDV

[LV07] Fabien Laguillaumie and Damien Vergnaud. Multi-designated verifiers signatures: anonymity without encryption. *Information Processing Letters*, 102(2–3):127–132, April 30, 2007. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lange:2002:PIE

[LW02] Tanja Lange and Arne Winterhof. Polynomial interpolation of the elliptic curve and XTR discrete logarithm. *Lecture Notes in Computer Science*, 2387:137–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2387/23870137.htm; http://link.springer-ny.com/link/service/series/

0558/papers/2387/23870137.pdf.

Lee:2004:IAK

[LW04] Narn-Yih Lee and Chien-Nan Wu. Improved authentication key exchange protocol without using one-way hash function. *Operating Systems Review*, 38(2):85–92, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Liang:2005:PAC

[LW05a] Wei Liang and Wenye Wang. On performance analysis of challenge/response based authentication in wireless networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 48(2):267–288, June 6, 2005. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Loepp:2005:PIC

[LW05b] Susan Loepp and William Wootters. *Protecting Information: From Classical Error Correction to Quantum Cryptography*. Cambridge University Press, Cambridge, UK, 2005. ISBN 0-521-82740-X (hardcover), 0-521-53476-3 (paperback). ???? pp. LCCN ????

Lyuu:2005:CIH

[LW05c] Yuh-Dauh Lyuu and Ming-Luen Wu. Cryptanalysis of and improvement on the Hwang–Chen multi-proxy multi-signature schemes. *Applied Mathematics and Computation*, 167(1):729–739, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lin:2000:PAS

[LWK00] Xiaodong Lin, Johnny W. Wong, and Weidong Kou. Performance analysis of secure Web server based on SSL. *Lecture Notes in Computer Science*, 1975: 249–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750249.htm; http://link.springer-ny.com/link/service/series/0558/papers/1975/19750249.pdf.

Lv:2005:PCA

[LWK05a] Jiqiang Lv, Xinmei Wang, and Kwangjo Kim. Practical convertible authenticated encryption schemes using self-certified public keys. *Applied Mathematics and Computation*, 169 (2):1285–1297, October 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lv:2005:SMS

[LWK05b] Jiqiang Lv, Xinmei Wang, and Kwangjo Kim. Security of a multisignature scheme for specified group of verifiers. *Applied Mathematics and Computation*, 166(1):58–63, July 6, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lin:2009:DMG

[LWL09] Song Lin, Biao Wang, and Zhoujun Li. Digital multisignature on the generalized conic curve over Z_n. *Computers & Security*, 28 (1–2):100–104, February/ March 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404808000801`.

Li:2005:IWR

[LWS05] Haifeng Li, Shuxun Wang, and Weiwei Song. Image watermarking resistant to global geometrical attacks. In Han et al. [HYZ05b], pages 911–?? ISBN 981-270-153-2. LCCN ???? URL `http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html`.

Lin:2005:NIB

[LWZH05] Chih-Yin Lin, Tzong-Chen Wu, Fangguo Zhang, and Jing-Jang Hwang. New identity-based society oriented signature schemes from pairings on elliptic curves. *Applied Mathematics and Computation*, 160(1):245–260, January 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Li:2007:PBS

[LXH07] F. Li, X. Xin, and Y. Hu. A pairing-based signcryption scheme using self-certified public keys. *International Journal of Computer Applications*, 29(3): 278–282, 2007. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2007.11441857`.

Lixin:2005:FLA

[LXM+05] Xu Lixin, Zhang Xincheng, He Min, Wu Xianglin, and Qingyun Ru. A four-layer architecture for Web application system security assurance: a safeguard mechanism research. In Han et al. [HYZ05b], pages 87–?? ISBN 981-270-153-2. LCCN ???? URL `http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html`.

Li:2005:AAU

[LY05] Zude Li and Xiaojun Ye. Attribute analysis of usage control (UCON). In Han et al. [HYZ05b], pages 59–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Li:2007:NBA

[LY07] Weihai Li and Yuan Yuan. A new blind attack procedure for DCT-based image encryption with spectrum learning. *International Journal of Image and Graphics (IJIG)*, 7(3):481–496, July 2007. CODEN ???? ISSN 0219-4678.

Lou:2002:ESA

[LYC02] D-C Lou, T-L Yin, and M-C Chang. An efficient steganographic approach. *International Journal of Computer Systems Science and Engineering*, 17(4/5):??, July/September 2002. CODEN CSSEEI. ISSN 0267-6192.

Liu:2007:IFW

[LYGL07] Shao-Hui Liu, Hong-Xun Yao, Wen Gao, and Yong-Liang Liu. An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. *Applied Mathematics and Computation*, 185(2):869–882, February 15, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lysyanskaya:2002:USV

[Lys02] Anna Lysyanskaya. Unique signatures and verifiable random functions from the DH–DDH separation. In Yung [Yun02a], pages 597–612. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420597.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420597.pdf.

Lysyanskaya:2007:AI

[Lys07] Anna Lysyanskaya. Authentication without identification. *IEEE Security & Privacy*, 5(3):69–71, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Lysyanskaya:2008:CHK

[Lys08] Anna Lysyanskaya. Cryptography: How to keep secrets safe. *Scientific American*, 299(3):88–95, September 2008. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v299/n3/full/scientificamerican0908-88.html; http://www.nature.com/scientificamerican/

journal/v299/n3/pdf/scientificamerican0908-88.pdf.

Leung:2001:WDI

[LZ01] K. H. Leung and Bing Zeng. Wavelet-domain image watermarking based on statistical metrics. *Lecture Notes in Computer Science*, 2195:788–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950788.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950788.pdf.

Li:2004:CAB

[LZ04] Hua Li and Chang N. Zhang. A cellular automata based reconfigurable architecture for hybrid cryptosystems. *The Computer Journal*, 47(3):320–328, May 2004. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Lao:2009:ORA

[LZ09] Yuanwei Lao and Yuan F. Zheng. Optimal rate allocation for logo watermarking. *International Journal of Image and Graphics (IJIG)*, 9 (1):1–25, January 2009. CODEN ???? ISSN 0219-4678.

Li:2001:GOT

[LZL+01] Zi-Chen Li, Jun-Mei Zhang, Jun Luo, William Song, and Yi-Qi Dai. Group-oriented (t, n) threshold digital signature schemes with traceable signers. *Lecture Notes in Computer Science*, 2040:57–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2040/20400057.htm; http://link.springer-ny.com/link/service/series/0558/papers/2040/20400057.pdf.

Li:2004:WMS

[LZP+04] Li Li, David Zhang, Zhigeng Pan, Jiaoying Shi, Kun Zhou, and Kai Ye. Watermarking 3D mesh by spherical parameterization. *Computers and Graphics*, 28(6): 981–989, December 2004. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic).

Michener:2000:IWM

[MA00a] John R. Michener and Tolga Acar. Internet watch: Managing system and active-content integrity. *Computer*, 33(7):108–110, July 2000. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co2000/pdf/r7108.pdf.

Michener:2000:MSA

[MA00b] John R. Michener and Tolga Acar. Managing system and active-content integrity. *Computer*, 33(7):108–110, July 2000. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Masuda:2002:CDC

[MA02] Naoki Masuda and Kazuyuki Aihara. Cryptosystems with discretized chaotic maps. *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, 49(1):28–40, 2002. CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic).

Maurer:2007:ICP

[MAA07] Ueli Maurer, Martin Abadi, and Ross Anderson. *Introduction to Cryptography: Principles and Applications*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-49244-5, 3-642-08040-5. 371 pp. LCCN QA76.9.A25.D447 2007eb.

Mrayati:2003:AKT

[MAaT03] M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. *Al-Kindi's treatise on cryptanalysis*, volume 1 of *Arabic origins of cryptology*. KFCRIS & KACST, Riyadh, Saudi Arabia, 2003. ISBN 9960-890-08-2. 204 pp. LCCN ????

Mrayati:2004:IAD

[MAaT04] M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. *Ibn 'ad-Durayhim's treatise on cryptanalysis*, volume 3 of *Arabic origins of cryptology*. KFCRIS & KACST, Riyadh, Saudi Arabia, 2004. ISBN 9960-890-20-0. 127 pp. LCCN ????

Mrayati:2005:IDB

[MAaT05] M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. *Ibn Dunaynir's book: Expositive chapters on cryptanalysis : (Maqasid al-fusul al-mutargima an hall at-targama)*, volume 4 of *Arabic origins of cryptology*. KFCRIS & KACST, Riyadh, Saudi Arabia, 2005. ISBN 9960-890-44-9. xii + 189 pp. LCCN ????

Mrayati:2006:TTC

[MAaT06] M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. *Three treatises on cryptanalysis of poetry*, volume 5 of *Arabic origins of cryptology*. KFCRIS & KACST, Riyadh, Saudi Arabia, 2006. ISBN 9960-890-56-2. x + 167 pp. LCCN ????

Mrayati:2007:TTC

[MAaT07] M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. *Two treatises on cryptanalysis: the two essays the treatise of ibn Wahab al-Ka tib*, volume 6 of *Arabic origins of cryptology*. KFCRIS & KACST, Riyadh, Saudi Arabia, 2007. ISBN 9960-893-58-8. xii + 125 pp. LCCN ????

Mrayati:20xx:AET

[MAaTxx] M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. *Analysis and editing of three Arabic manuscripts: Al-Kindi, Ibn-Adlan, Ibn-Al-Durahim*. Origins of Arab cryptography and cryptanalysis. KFCRIS & KACST, Riyadh, Saudi Arabia, 20xx. ISBN ???? ???? pp. LCCN ???? Introduction by Chaker Faham.

McDaniel:2006:OAI

[MABI06] Patrick McDaniel, William Aiello, Kevin Butler, and John Ioannidis. Origin authentication in interdomain routing. *Computer Networks (Amsterdam, Netherlands: 1999)*, 50(16):2953–2980, November 14, 2006. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Machado:2000:NCP

[Mac00] Alexis Warner Machado. The Nimbus cipher: a proposal for NESSIE. Report ??, ????, ????, September 2000.

MacKenzie:2001:MEP

[Mac01] Philip MacKenzie. More efficient password-authenticated key exchange. *Lecture Notes in Computer Science*, 2020:361–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200361.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200361.pdf`.

Mohay:2003:CIF

[MAC+03] George M. Mohay, Alison Anderson, Byron Collie, Olivier de Vel, and Rod McKemmish, editors. *Computer and intrusion forensics*. Artech House computer security series. Artech House Inc., Norwood, MA, USA, 2003. ISBN 1-58053-369-8. xxi + 395 pp. LCCN QA76.9.A25 C628 2003.

Madsen:2000:HCI

[Mad00a] Wayne Madsen. Health care industry debate: Electronic versus digital signatures. *Network Security*, 2000(12):5, December 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485800120136`.

Madsen:2000:RDU

[Mad00b] Wayne Madsen. Revised draft US crypto export regulations leaked. *Network Security*, 2000(3):8, March 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800880241.

Madsen:2000:WUN

[Mad00c] Wayne Madsen. Whitehouse unveils new cybercrime, crypto export policies. *Network Security*, 2000 (8):7, August 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348580008017X.

Madsen:2004:FFD

[Mad04] Wayne Madsen. Former FBI Director says encryption fuels terrorists. *Network Security*, 2004(4):1, 3, April 2004. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485804000595.

Mahle:2004:DDI

[Mah04] Melissa Boyle Mahle. *Denial and deception: an insider's view of the CIA from Iran–Contra to 9/11*. Nation Books, New York, NY, USA, 2004. ISBN 1-56025-649-4. xi + 403 pp. LCCN JK468.I6 M333 2004.

Malcolm:2002:LAM

[Mal02] James Malcolm. Lightweight authentication in a mobile network (transcript of discussion). *Lecture Notes in Computer Science*, 2467: 217–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2467/24670217.htm; http://link.springer.de/link/service/series/0558/papers/2467/24670217.pdf.

Maloof:2006:MLD

[Mal06] Marcus A. Maloof, editor. *Machine learning and data mining for computer security: methods and applications*. Advance information knowledge processing. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 1-84628-029-X. xvi + 210 pp. LCCN QA76.9.A25 M29 2006.

Manger:2001:CCA

[Man01] James Manger. A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS #1 v2.0. In Kilian [Kil01a], pages 230–?? ISBN 3-540-42456-3 (paperback). LCCN

QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390230.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390230.pdf.

Mann:2002:HI

[Man02] Charles C. Mann. Homeland insecurity. *The Atlantic*, ??(??):??, September 2002. URL http://www.theatlantic.com/issues/2002/09/mann.htm.

Mann:2008:HHS

[Man08] Ian Mann. *Hacking the human: social engineering techniques and security countermeasures*. Gower, Aldershot, England, 2008. ISBN 0-566-08773-1. vii + 254 pp. LCCN HM668 .M36 2008. URL http://www.loc.gov/catdir/toc/ecip0817/2008019977.html.

Mao:2001:TRC

[Mao01] Wenbo Mao. Timed-release cryptography. *Lecture Notes in Computer Science*, 2259: 342–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590342.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590342.pdf.

Mao:2004:MCT

[Mao04] Wenbo Mao. *Modern Cryptography: Theory and Practice*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 2004. ISBN 0-13-066943-1, 0-13-288741-X (on-demand digital reprint). xxxviii + 707 pp. LCCN ???? US$54.99.

Marques:2002:BSJ

[Mar02a] Paulo Marques. Building secure Java RMI servers. *Dr. Dobb's Journal of Software Tools*, 27(11):36, 38, 40–42, 44, November 2002. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/documents/s=7644/ddj0211d/.

Martinelli:2002:SSA

[Mar02b] Fabio Martinelli. Symbolic semantics and analysis for crypto-CCS with (almost) generic inference systems. *Lecture Notes in Computer Science*, 2420: 519–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2420/24200519.htm; http://link.springer.de/link/service/series/0558/papers/2420/24200519.pdf.

Mares:2005:BRA

[Mar05a] Peter Mares. Book review: *Art of Java Web Development*, by N. Ford. *The Computer Journal*, 48(2): 253, March 2005. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/free_pdf/bxh071.pdf; http://www3.oup.co.uk/computer_journal/hdb/Volume_48/Issue_02/bxh071.sgm.abs.html.

Martin:2005:STA

[Mar05b] Thomas Martin. *A set theoretic approach to broadcast encryption*. Thesis (Ph.D.), University of London, London, UK, 2005. 235 pp.

Martin:2007:SCE

[Mar07] Keye Martin. Secure communication without encryption? *IEEE Security & Privacy*, 5(2):68–71, March/April 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Martin:2008:CCI

[Mar08a] Luther Martin. Crypto corner: Identity-based encryption and beyond. *IEEE Security & Privacy*, 6(5): 62–64, September/October 2008. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Martin:2008:IBE

[Mar08b] Luther Martin. Identity-based encryption comes of age. *Computer*, 41(8):93–95, August 2008. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Mastroeni:2004:APA

[Mas04] Isabella Mastroeni. Algebraic power analysis by abstract interpretation. *Higher-Order and Symbolic Computation*, 17(4):297–345, December 2004. CODEN LSCOEX. ISSN 1388-3690 (print), 2212-0793 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1388-3690&volume=17&issue=4&spage=297.

Matsui:2002:FSE

[Mat02] Mitsuru Matsui, editor. *Fast software encryption: 8th International Workshop, FSE 2001, Yokohama, Japan, April 2–4, 2001: Revised Papers*, volume 2355 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-43869-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F77 2002. URL http://link.springer-ny.com/

link/service/series/0558/tocs/t2355.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2355.

Mathieson:2005:UCR

[Mat05] SA Mathieson. UK crypto regulation option dies. *Network Security*, 2005(6): 2, June 2005. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485805702415.

Maurer:2001:C

[Mau01] Ueli Maurer. Cryptography 2000 ± 10. *Lecture Notes in Computer Science*, 2000:63–85, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2000/20000063.htm; http://link.springer-ny.com/link/service/series/0558/papers/2000/20000063.pdf.

Maurer:2004:RCD

[Mau04] Ueli Maurer. The role of cryptography in database security. In ACM [ACM04a], pages 5–10. ISBN 1-58113-859-8. LCCN QA76.9.D3.

Maughan:2005:HSC

[Mau05] Douglas Maughan. Homeland security: cyber security R&D initiatives. In Meadows and Syverson [MS05b], page 1. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Maximov:2006:SWC

[Max06] Alexander Maximov. *Some words on cryptanalysis of stream ciphers*. Department of Information Technology, Lund University, Lund, Sweden, 2006. ISBN 91-7167-039-4. xiv + 242 pp. LCCN ????

Mayers:2001:USQ

[May01] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, May 2001. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL http://www.acm.org/pubs/citations/journals/jacm/2001-48-3/p351-mayers/.

May:2002:CUR

[May02] Alexander May. Cryptanalysis of unbalanced RSA with small CRT-exponent. In Yung [Yun02a], pages 242–256. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420242.htm; http://link.springer.de/link/

service/series/0558/papers/2442/24420242.pdf.

May:2004:CRS

[May04] Alexander May. Computing the RSA secret key is deterministic polynomial time equivalent to factoring. In Franklin [Fra04], pages 213–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

May:2009:PIS

[May09] John P. May, editor. *Proceedings of the 2009 international symposium on Symbolic and algebraic computation, KIAS, Seoul, Korea, July 28–31, 2009*. ACM Press, New York, NY 10036, USA, 2009. ISBN 1-60558-609-9. LCCN ????

Mel:2001:CD

[MB01] H. X. Mel and Doris M. Baker. *Cryptography Decrypted*. Addison-Wesley, Reading, MA, USA, 2001. ISBN 0-201-61647-5. xx + 352 pp. LCCN QA76.9.A25 M44 2001. US $29.95; CDN $44.95; UK£22.99.

Mohanty:2008:IWB

[MB08] Saraju P. Mohanty and Bharat K. Bhargava. Invisible watermarking based on creation and robust insertion-extraction of image adaptive watermarks. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 5(2):12:1–12:??, November 2008. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

McKinnon:2004:CCS

[MBS04] A. David McKinnon, David E. Bakken, and John C. Shovic. A configurable cryptography subsystem in a middleware framework for embedded systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 46(6):771–795, December 20, 2004. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Montenegro:2004:CBI

[MC04] Gabriel Montenegro and Claude Castelluccia. Crypto-based identifiers (CBIDs): Concepts and applications. *ACM Transactions on Information and System Security*, 7(1):97–127, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

McAndrew:2008:TCO

[McA08] Alasdair McAndrew. Teaching cryptography with open-source software. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 40(1): 325–329, March 2008. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). Proceedings of SIGCSE 08.

McElheny:2004:TPW

[McE04] Victor K. McElheny. *Tuxedo Park: A Wall Street Tycoon and the Secret Palace of Science that Changed the Course of World War II* (review). *Technology and Culture*, 45(2):456–457, April 2004. CODEN TECUA3. ISSN 0040-165X (print), 1097-3729 (electronic). URL https://muse.jhu.edu/pub/1/article/55675.

McGraw:2006:SSB

[McG06] Gary McGraw. *Software security: building security in*. Addison-Wesley software security series. Addison-Wesley, Reading, MA, USA, 2006. ISBN 0-321-35670-5 (paperback). xxxvi + 408 pp. LCCN QA76.9.A25 M4286 2006. URL http://www.loc.gov/catdir/toc/ecip062/2005031598.html.

Myles:2005:ETS

[MCHN05] Ginger Myles, Christian Collberg, Zachary Heidepriem, and Armand Navabi. The evaluation of two software watermarking algorithms. *Software—Practice and Experience*, 35(10):923–938, August 2005. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

McKenna:2004:EAE

[McK04] Brian McKenna. Erratum to "Attacks on the (enhanced) Yang–Shieh authentication" [Comput Secur **22**(8) (2003) 725–727]. *Computers & Security*, 23 (1):85, February 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804000082. See [CZ03].

McLaughlin:2006:PZW

[McL06] Laurianne McLaughlin. Philip Zimmermann on What's Next after PGP? *IEEE Security & Privacy*, 4(1):10–13, January/February 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://ieeexplore.ieee.org/iel5/8013/33481/01588818.pdf; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=33481&arnumber=1588818.

McNichol:2003:HTM

[McN03] Tom McNichol. How two

math geeks with a lava lamp and a webcam are about to unleash chaos on the Internet. *Wired*, 11(8):??, August 2003. CODEN WREDEM. ISSN 1059-1028 (print), 1078-3148 (electronic). URL `http://www.lavarnd.org; http://www.wired.com/wired/archive/11.08/random.html`.

Martin:2004:AMC

[MD04] Cynthia E. Martin and Jeffrey H. Dunn. Authentication mechanisms for call control message integrity and origin verification. *Bell Labs Technical Journal*, 8 (4):71–91, Winter 2004. CODEN BLTJFD. ISSN 1089-7089 (print), 1538-7305 (electronic).

Macchetti:2005:QPH

[MD05] Marco Macchetti and Luigi Dadda. Quasi-pipelined hash circuits. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL `http://arith17.polito.it/final/paper-149.pdf`.

McCamant:2008:QIF

[ME08a] Stephen McCamant and Michael D. Ernst. Quantitative information flow as network flow capacity. *ACM SIGPLAN Notices*, 43(6): 193–205, June 2008. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Monteiro:2008:AVM

[ME08b] Steena D. S. Monteiro and Robert F. Erbacher. An authentication and validation mechanism for analyzing syslogs forensically. *Operating Systems Review*, 42(3): 41–50, April 2008. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Meadows:2001:OIF

[Mea01] Catherine Meadows. Open issues in formal methods for cryptographic protocol analysis. *Lecture Notes in Computer Science*, 2052: 21–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2052/20520021.htm; http://link.springer-ny.com/link/service/series/0558/papers/2052/20520021.pdf`.

Meadows:2004:OSM

[Mea04] Catherine Meadows. Ordering from Satan's menu: a survey of requirements specification for formal analysis of cryptographic protocols. *Science of Computer Programming*, 50(1–3):3–22, March 2004. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic).

Mehrabi:2001:DW

[Meh01] Hamid Reza Mehrabi. Digital watermark. *Lecture Notes in Computer Science*, 2163:49–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2163/21630049.htm; http://link.springer-ny.com/link/service/series/0558/papers/2163/21630049.pdf.

Mena:2003:IDM

[Men03] Jesús Mena. *Investigative data mining for security and criminal detection*. Butterworth-Heinemann, Boston, MA, USA, 2003. ISBN 0-7506-7613-2. xvi + 452 pp. LCCN QA76.9.D343 M44 2003. US$49.95.

Menezes:2005:TCC

[Men05] Alfred Menezes, editor. *Topics in cryptology CT-RSA 2005: The cryptographers' track at the RSA Conference 2005, San Francisco, CA, USA, February 14–18, 2005. Proceedings*, volume 3376 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-24399-2 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 R753 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3376; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b105222.

Menezes:2007:ACC

[Men07] A. J. (Alfred J.) Menezes, editor. *Advances in cryptology — CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2007: proceedings*, volume 4622 of *Lecture notes in computer science, 0302-9743*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-74142-9 (paperback). LCCN QA76.9.A25 C79 2007. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=4622.

Messerges:2000:SAF

[Mes00] Thomas Messerges. Securing the AES finalists against power analysis attacks (abstract only). In NIST [NIS00], page 10. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/

aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Messerges:2001:SAF

[Mes01] Thomas S. Messerges. Securing the AES finalists against power analysis attacks. *Lecture Notes in Computer Science*, 1978: 150–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780150.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780150.pdf.

McGrew:2001:AAE

[MF01] David A. McGrew and Scott R. Fluhrer. Attacks on additive encryption of redundant plaintext and implications on Internet security. In *Selected areas in cryptography (Waterloo, ON, 2000)*, volume 2012 of *Lecture Notes in Comput. Sci.*, pages 14–28. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120014.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120014.pdf.

Marti-Farre:2007:NSS

[MF07] Jaume Martí-Farré. A note on secret sharing schemes with three homogeneous access structure. *Information Processing Letters*, 102 (4):133–137, May 16, 2007. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Millan:2004:NCE

[MFD04] William Millan, Joanne Fuller, and Ed Dawson. New concepts in evolutionary search for Boolean functions in cryptology. *Computational Intelligence*, 20 (3):463–474, August 2004. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Matula:2005:TLS

[MFFT05] David Matula, Alex Fit-Florea, and Mitchell Thornton. Table lookup structures for multiplicative inverses modulo 2^k. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL http://arith17.polito.it/final/paper-160.pdf.

Mueller:2006:SMG

[MFK+06] Maik Mueller, Michael Freidrich, Klaus Kiefer, Ralf Miko, and Juergen Schneider. System and method for generating pseudo-random numbers. United States Patent 7,894,602., March 31, 2006. URL http:www.google.com/patents/US7894602.

Muller:2009:BPE

[MFS+09] Christoph Müller, Steffen Frey, Magnus Strengert, Carsten Dachsbacher, and Thomas Ertl. Best paper of EGPGV — Eurographics Symposium on Parallel Graphics and Visualization, Guest Editor Jean Favre: a compute unified system architecture for graphics clusters incorporating data locality. *IEEE Transactions on Visualization and Computer Graphics*, 15(4):605–617, July/August 2009. CODEN ITVGEA. ISSN 1077-2626 (print), 1941-0506 (electronic), 2160-9306.

Minier:2001:SCC

[MG01] Marine Minier and Henri Gilbert. Stochastic cryptanalysis of Crypton. *Lecture Notes in Computer Science*, 1978:121–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780121.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780121.pdf.

Muresan:2008:PCA

[MG08] R. Muresan and S. Gregori. Protection circuit against differential power analysis attacks for smart cards. *IEEE Transactions on Computers*, 57(11):1540–1549, November 2008. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4585359.

Mukherjee:2002:CAB

[MGC02] Monalisa Mukherjee, Niloy Ganguly, and P. Pal Chaudhuri. Cellular automata based authentication (CAA). *Lecture Notes in Computer Science*, 2493:259–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2493/24930259.htm; http://link.springer.de/link/service/series/0558/papers/2493/24930259.pdf.

Molland:2004:ICA

[MH04] Håvard Molland and Tor

Helleseth. An improved correlation attack against irregular clocked and filtered keystream generators. In Franklin [Fra04], pages 373–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Ma:2005:NCD

[MH05] Yiping Ma and Jiqing Han. A new capability description for audio information hiding. In Han et al. [HYZ05b], pages 65–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Maas:2009:SRW

[MH09] Ad Maas and Hans Hooijmaijers. *Scientific research in World War II: what scientists did in the war*. Routledge studies in modern history. Routledge/Taylor and Francis, New York, NY, 2009. ISBN 0-203-88318-7 (e-book), 0-7103-1340-3 (hardcover). xii + 240 pp. LCCN Q141 .H195 2009. URL http://www.loc.gov/catdir/toc/ecip0824/2008033118.html.

Moon:2002:IDC

[MHL+02] Dukjae Moon, Kyungdeok Hwang, Wonil Lee, Sangjin Lee, and Jongin Lim. Impossible differential cryptanalysis of reduced round XTEA and TEA. *Lecture Notes in Computer Science*, 2365:49–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650049.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650049.pdf.

May:2002:SKS

[MHM+02] Lauren May, Matt Henricksen, William Millan, Gary Carter, and Ed Dawson. Strengthening the key schedule of the AES. *Lecture Notes in Computer Science*, 2384:226–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840226.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840226.pdf.

Mihaljevic:2009:ASC

[MI09] Miodrag J. Mihaljević and Hideki Imai. An approach for stream ciphers design based on joint computing over random and secret data. *Computing*, 85(1–2): 153–168, June 2009. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=85&issue=1&spage=153.

Micciancio:2001:ILB

[Mic01] Daniele Micciancio. Improving lattice based cryptosystems using the Hermite normal form. *Lecture Notes in Computer Science*, 2146: 126–145, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Micciancio:2002:GCK

[Mic02a] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In IEEE [IEE02], pages 356–365. CODEN ASFPDV. ISBN 0-7695-1822-2. ISSN 0272-5428. LCCN QA267. URL http://ieeexplore.ieee.org/iel5/8411/26517/01181960.pdf?isnumber=26517&prod=CNF&arnumber=1181960&arSt=+356&ared=+365&arAuthor=Micciancio%2C+D.; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=26517&arnumber=1181960&count=82&index=36. IEEE Computer Society Order Number PR01822.

Micciancio:2002:ICH

[Mic02b] Daniele Micciancio. Improved cryptographic hash functions with worst-case/average-case connection. In ACM [ACM02], pages 609–618. ISBN 1-58113-495-9. LCCN QA75.5 .A22 2002. ACM order number 508020.

Millen:2003:FD

[Mil03] Jonathan Millen. On the freedom of decryption. *Information Processing Letters*, 86(6):329–333, June 30, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Minkel:2003:CTT

[Min03] J. R. Minkel. Could trapping tiny ions crack the toughest codes? *IEEE Spectrum*, 40(3):31–32, March 2003. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Mironov:2002:RSO

[Mir02] Ilya Mironov. (not so) random shuffles of RC4. In Yung [Yun02a], pages 304–319. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Mirkovic:2005:IDS

[Mir05] Jelena Mirkovic, editor. *Internet denial of service: attack and defense mechanisms*. The Radia Perlman series in computer networking and security. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 2005. ISBN 0-13-147573-8 (paperback). xxii + 372 pp. LCCN TK5105.59 .I5455 2004. URL http://www.loc.gov/catdir/toc/ecip0422/2004020335.html.

Mishra:2006:PCS

[Mis06] P. M. Mishra. Pipelined computation of scalar multiplication in elliptic curve cryptosystems (extended version). *IEEE Transactions on Computers*, 55(8):1000–1010, August 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1650197.

Misic:2008:TEC

[Miš08] Jelena Mišić. Traffic and energy consumption of an IEEE 802.15.4 network in the presence of authenticated, ECC Diffie–Hellman ephemeral key exchange. *Computer Networks (Amsterdam, Netherlands: 1999)*, 52(11):2227–2236, August 8, 2008. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Mitchell:2000:MSN

[Mit00] Chris J. Mitchell. Making serial number based authentication robust against loss of state. *Operating Systems Review*, 34(3):56–59, July 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Mitra:2002:TAD

[Mit02a] Ananda Mitra. Trust, authenticity, and discursive power in cyberspace. *Communications of the Association for Computing Machinery*, 45(3):27–29, March 2002. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Mitrakas:2002:CCI

[Mit02b] Andreas Mitrakas. Citizen centric identity management: Chip tricks? *Network Security*, 2002(7):15–16, July 1, 2002. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S1353485802070101.

Miyazaki:2001:ISG

[Miy01] Takeru Miyazaki. An improved scheme of the Gennaro-Krawczyk-Rabin undeniable signature system based on RSA. *Lecture Notes in Computer Science*, 2015:135–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2015/20150135.htm; http://link.springer-ny.com/link/service/series/0558/papers/2015/20150135.pdf.

MacDonald:2003:CDS

[MJ03] Matthew MacDonald and Erik Johansson. *C# data security handbook*. Wrox Press, Chicago, IL, USA, 2003. ISBN 1-86100-801-5 (paperback). vii + 356 pp. LCCN ????

Maltoni:2004:BAE

[MJ04] Davide Maltoni and Anil K. Jain, editors. *Biometric Authentication: ECCV 2004 International Workshop, BioAW 2004, Prague, Czech Republic, May 15th, 2004: Proceedings*, volume 3087 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22499-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.P3E27 2004. URL http://link.springer-ny.com/link/service/series/0558/tocs/t3087.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3087; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99174.

Moore:2001:AGK

[MJD01] Patrick C. Moore, Wilbur R. Johnson, and Richard J. Detry. Adapting Globus and Kerberos for a secure ASCI grid. In ACM [ACM01b], page ?? ISBN 1-58113-293-X. LCCN ???? URL http://www.sc2001.org/papers/pap.pap192.pdf.

Mabry:2007:USE

[MJF07] Frank J. Mabry, John R. James, and Aaron J. Ferguson. Unicode steganographic exploits: Maintaining enterprise border security. *IEEE Security & Privacy*, 5(5):32–39, September/October 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Mandviwalla:2008:MBW

[MJF+08] Munir Mandviwalla, Abhijit Jain, Julie Fesenmaier, Jeff Smith, Paul Weinberg, and Greg Meyers. Municipal broadband wireless networks. *Communications of the Association for Computing Machinery*, 51(2):72–80, February 2008. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Moffie:2005:AAS

[MK05a] Micha Moffie and David Kaeli. ASM: application security monitor. *ACM SIGARCH Computer Architecture News*, 33(5):21–26, December 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Moyle:2005:CLD

[MK05b] Ed Moyle and Diana Kelley. *Cryptographic libraries for developers*. Charles River Media, Hingham, MA, USA, 2005. ISBN 1-58450-409-9. ???? pp. LCCN QA76.76.D47 M72 2005. URL http://www.loc.gov/catdir/toc/ecip0519/2005026626.html.

Mazieres:2000:SKM

[MKKW00] David Mazières, Michael Kaminsky, M. Frans Kaashoek, and Emmett Witchel. Separating key management from file system security. *Operating Systems Review*, 34(2):19–20, April 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Majzoobi:2009:TDI

[MKP09] Mehrdad Majzoobi, Farinaz Koushanfar, and Miodrag Potkonjak. Techniques for design and implementation of secure reconfigurable PUFs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 2(1):5:1–5:??, March 2009. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

McDonald:2008:SID

[MKY08] J. Todd McDonald, Yong C. Kim, and Alec Yasinsac. Software issues in digital forensics. *Operating Systems Review*, 42(3):29–40, April 2008. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

McGregor:2005:PCK

[ML05] John P. McGregor and Ruby B. Lee. Protecting cryptographic keys and computations via virtual secure coprocessing. *ACM SIGARCH Computer Architecture News*, 33(1):16–26, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Miaou:2001:BCW

[MLC01] Shaou-Gang Miaou, Tzung-Shian Lee, and Chih-Ming Chen. BCH coded watermarks for error-prone transmission of MPEG video. *Lecture Notes in Computer Science*, 2195: 654–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950654.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950654.pdf.

Malone-Lee:2003:TBO

[MLM03] John Malone-Lee and Wenbo Mao. Two birds one stone: Signcryption using RSA. In Joye [Joy03b], pages 211–225. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Maitra:2001:SDD

[MM01a] S. Maitra and D. P. Mukherjee. Spatial domain digital watermarking with buyer authentication. *Lecture Notes in Computer Science*, 2247:149–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470149.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470149.pdf.

McLoone:2001:HPS

[MM01b] M. McLoone and J. V. McCanny. High performance single-chip FPGA Rijndael algorithm implementations. *Lecture Notes in Computer Science*, 2162: 65–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620065.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620065.pdf.

McLoone:2001:SCF

[MM01c] Máire McLoone and John V. McCanny. Single-chip FPGA implementation of the advanced encryption standard algorithm. *Lecture Notes in Computer Science*, 2147:152–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2147/21470152.htm; http://link.springer-ny.com/link/service/series/0558/papers/2147/21470152.pdf.

Mana:2002:PMD

[MM02] Antonio Maña and Sonia Matamoros. Practical mobile digital signatures. *Lecture Notes in Computer Science*, 2455: 224–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2455/24550224.htm; http://link.springer-ny.com/link/service/series/0558/papers/2455/24550224.pdf.

Moldovyan:2007:IC

[MM07a] Nick Moldovyan and Alex Moldovyan. *Innovative cryptography*. Charles River Media programming series. Charles River Media, Boston, MA, USA, second edition, 2007. ISBN 1-58450-467-6 (paperback). xiii + 386 pp. LCCN QA76.9.A25 M665 2007. URL http://www.loc.gov/catdir/toc/ecip0611/2006009839.html.

Mullen:2007:FFA

[MM07b] Gary L. Mullen and Carl Mummert. *Finite Fields and Applications*, volume 41 of *Student mathematical library*. American Mathematical Society, Providence, RI, USA, 2007. ISBN 0-8218-4418-0 (paperback). ix + 175 pp. LCCN QA247.3 .M85 2007.

Moreira:2002:RCE

[MMH02] Emmanuel A. Moreira, Paul L. McAlpine, and Simon D. Haynes. Rijndael cryptographic engine on the UltraSONIC reconfigurable platform. *Lecture Notes in Computer Science*, 2438:770–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2438/24380770.htm; http://link.springer-ny.com/link/service/series/0558/papers/2438/24380770.pdf.

Milenkovic:2005:UIB

[MMJ05] Milena Milenković, Aleksandar Milenković, and Emil Jovanov. Using instruction block signatures to counter code injection attacks. *ACM SIGARCH Computer Architecture News*, 33(1):108–117, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Maltoni:2003:HFR

[MMJP03] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Springer professional computing. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 0-387-95431-7. xii + 348 pp. LCCN HV6074 .H25 2003. US$59.95. Includes DVD-ROM.

McEvoy:2009:IWH

[MMMT09] Robert P. McEvoy, Colin C. Murphy, William P. Marnane, and Michael Tunstall. Isolated WDDL: a hiding countermeasure for differential power analysis on FPGAs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 2(1):3:1–3:??, March 2009. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Maitra:2006:PCI

[MMV06] Subhamoy Maitra, C. E. Veni Madhavan, and Ramarathnam Venkatesan, editors. *Progress in Cryptology — INDOCRYPT 2005: 6th International Conference on Cryptology in India, Bangalore, India, December 10–12, 2005. Proceedings*, volume 3797 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-30805-9 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3797.

Matsumoto:2002:IAG

[MMYH02] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Proceedings of SPIE: Optical Security and Counterfeit Deterrence Techniques IV, 2002*, volume 4677, page ?? Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 2002. URL http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf.

Maclean:2000:OIG

[MMZ00] Abby Maclean, Stephen M. Matyas, and Nevenko Zunic. Organization implementation guidelines for recovery of encrypted information. *Computers & Security*, 19(1):69–81, January 1, 2000. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://

www.sciencedirect.com/science/article/pii/S0167404800863658.

Mizuki:2001:NSN

[MN01] Takaaki Mizuki and Takao Nishizeki. Necessary and sufficient numbers of cards for sharing secret keys on hierarchical groups. *Lecture Notes in Computer Science*, 2223:196–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2223/22230196.htm; http://link.springer-ny.com/link/service/series/0558/papers/2223/22230196.pdf.

Mercuri:2003:IRS

[MN03] Rebecca T. Mercuri and Peter G. Neumann. Inside risks: Security by obscurity. *Communications of the Association for Computing Machinery*, 46(11):160, November 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Mukhopadhyay:2014:EMP

[MN14] Debapriyay Mukhopadhyay and Subhas C. Nandy. Efficient multiple-precision integer division algorithm. *Information Processing Letters*, 114(3):152–157, March 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013002627. This paper provides a correction to the algorithm presented in [HZSL05], and also supplies a complicated correctness proof.

Martel:2004:GMA

[MND+04] Charles Martel, Glen Nuckolls, Premkumar Devanbu, Michael Gertz, April Kwong, and Stuart G. Stubblebine. A general model for authenticated data structures. *Algorithmica*, 39(1):21–41, January 2004. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=39&issue=1&spage=21.

Martinez-Nadal:2002:CUM

[MNFG02] Apol·lònia Martínez-Nadal and Josep Lluís Ferrer-Gomila. Comments to the UNCITRAL model law on electronic signatures. *Lecture Notes in Computer Science*, 2433:229–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330229.htm; http://link.springer-

ny.com/link/service/series/0558/papers/2433/24330229.pdf.

Meyer:2001:FIC

[MNP01] Andreas Meyer, Stefan Neis, and Thomas Pfahler. First implementation of cryptographic protocols based on algebraic number fields. *Lecture Notes in Computer Science*, 2119:84–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190084.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190084.pdf.

Monsignori:2001:WMS

[MNS01] M. Monsignori, P. Nesi, and M. B. Spinu. Watermarking music sheets. *Lecture Notes in Computer Science*, 2195:646–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950646.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950646.pdf.

Mironov:2008:SAE

[MNS08] Ilya Mironov, Moni Naor, and Gil Segev. Sketching in adversarial environments. In ACM [ACM08], pages 651–660. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

MacAndrew:2000:LPT

[MNT+00] Tim MacAndrew, Robert H. Norman, Jeff Templon, Kevin W. Wall, Shari Lawrence Pfleeger, Joseph C. Sligo, Christopher Jack, and Terry Ritter. Letters: Probability theory and software engineering; food for thought; uncovering erroneous assumptions; Einstein's Nobel Prize; small-project process improvement; the truth about cryptography. *Computer*, 33(2):4–8, February 2000. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co2000/pdf/r2004.pdf.

Mykletun:2006:AIO

[MNT06] Einar Mykletun, Maithili Narasimha, and Gene Tsudik. Authentication and integrity in outsourced databases. *ACM Transactions on Storage*, 2(2):107–138, May 2006. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Mollin:2001:IC

[Mol01] Richard A. Mollin. *An Introduction to Cryptography*. The CRC Press series on discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, 2001. ISBN 1-58488-127-5. xiii + 373 pp. LCCN QA268 .M65 2000. UK£29.99.

Moller:2002:PEC

[Möl02] Bodo Möller. Parallelizable elliptic curve point multiplication method with resistance against side-channel attacks. *Lecture Notes in Computer Science*, 2433: 402–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330402.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330402.pdf.

Moller:2003:PSP

[Möl03a] Bodo Möller. Provably secure public-key encryption for length-preserving Chaumian mixes. In Joye [Joy03b], pages 244–262. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Mollin:2003:RPK

[Mol03b] Richard A. Mollin. *RSA and Public-Key Cryptography*. Chapman and Hall/CRC, Boca Raton, FL, USA, 2003. ISBN 1-58488-338-3. xii + 291 pp. LCCN QA268 .M655 2003. US$79.95.

Mollin:2005:CGS

[Mol05] Richard A. Mollin. *Codes: the guide to secrecy from ancient to modern times*. Chapman and Hall/CRC, Boca Raton, FL, USA, 2005. ISBN 1-58488-470-3. xx + 678 pp. LCCN QA76.9.A25 M67 2005. URL http://www.loc.gov/catdir/enhancements/fy0647/2005041403-d.html.

Mollin:2007:IC

[Mol07] Richard A. Mollin. *An introduction to cryptography*. Discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, second edition, 2007. ISBN 1-58488-618-8. x + 413 pp. LCCN QA268 .M65 2007. URL http://www.loc.gov/catdir/enhancements/fy0664/2006049639-d.html.

Monniaux:2003:ACP

[Mon03] David Monniaux. Abstracting cryptographic protocols with tree automata.

Science of Computer Programming, 47(2–3):177–202, May/June 2003. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic).

Moore:2001:UMW

[Moo01] Samuel K. Moore. Unhooking medicine [wireless networking]. *IEEE Spectrum*, 38(1):107–108, January 2001. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Moore:2007:CQK

[Moo07] Samuel K. Moore. Commercializing quantum keys. *IEEE Spectrum*, 44(3):15–17, March 2007. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Mangard:2006:PAA

[MOP06] Stephan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks and Countermeasures for Cryptographic Smart Cards*, volume 450 of *Advances in Information Security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 0-387-30857-1. 250 (est) pp. LCCN ???? URL `http://deposit.ddb.de/cgi-bin/dokserv?id=2739575&prov=M&dok_var=1&dok_ext=htm`.

Morris:2003:KKL

[Mor03] James Morris. Kernel korner: The Linux kernel cryptographic API. *Linux Journal*, 108:??, April 2003. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Moritz:2005:KAE

[Mor05] Hannes Moritz. Kryptoanalyse des Advanced Encryption Standard. (German) [cryptanalysis of the Advanced Encryption Standard]. Diplom-Arbeit, Technische Universität Wien, Wien, Austria, 2005. iii + 116 pp.

Moses:2006:DSD

[Mos06] Phil Moses. Demons seeking dæmons—a practical approach to hardening your openSSH configuration. *Linux Journal*, 2006(143):3, March 2006. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Merton:2000:NBG

[MP00] Orren Merton and Linda Dailey Paulson. News briefs: Gamers jump into broadband technology; Intel has new chip design for handhelds; patent expiration begins new encryption era; privacy organization raises privacy concerns. *Computer*, 33(11):16–19, November 2000. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co2000/pdf/ry016.pdf.

McMillan:2001:JIA

[MP01a] Scott McMillan and Cameron Patterson. JBits^{TM} implementations of the Advanced Encryption Standard (Rijndael). *Lecture Notes in Computer Science*, 2147:162–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2147/21470162.htm; http://link.springer-ny.com/link/service/series/0558/papers/2147/21470162.pdf.

Mihailescu:2001:BRE

[MP01b] Preda Mihailescu and F. Pappalardi. Book review: *Elliptic curves in cryptography*. *Mathematics of Computation*, 70(236):1755–1759, October 2001. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2001-70-236/S0025-5718-01-01400-4/bookrev-S0025-5718-01-01400-4.html; http://www.ams.org/mcom/2001-70-236/S0025-5718-01-01400-4/S0025-5718-01-01400-4.dvi; http://www.ams.org/mcom/2001-70-236/S0025-5718-01-01400-4/S0025-5718-01-01400-4.pdf; http://www.ams.org/mcom/2001-70-236/S0025-5718-01-01400-4/S0025-5718-01-01400-4.ps; http://www.ams.org/mcom/2001-70-236/S0025-5718-01-01400-4/S0025-5718-01-01400-4.tex.

Moshopoulos:2001:NSA

[MP01c] Nikos K. Moshopoulos and K. Z. Pekmestzi. A novel systolic architecture for an efficient RSA implementation. *Lecture Notes in Computer Science*, 1992:416–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920416.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920416.pdf.

Malkhi:2002:ACE

[MP02] Dahlia Malkhi and Elan Pavlov. Anonymity without 'cryptography' (extended abstract). *Lecture Notes in Computer Science*, 2339:117–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/

bibs/2339/23390117.htm; http://link.springer-ny.com/link/service/series/0558/papers/2339/23390117.pdf.

Maurer:2003:SMR

[MP03] Ueli Maurer and Krzysztof Pietrzak. The security of many-round Luby–Rackoff pseudo-random permutations. *Lecture Notes in Computer Science*, 2656: 544–561, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_34.pdf.

Micciancio:2005:ASS

[MP05] Daniele Micciancio and Saurabh Panjwani. Adaptive security of symbolic encryption. In Kilian [Kil05], pages 169–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Matusiewicz:2006:FGD

[MP06] Krystian Matusiewicz and Josef Pieprzyk. Finding good differential patterns for attacks on SHA-1. In Ytrehus [Ytr06], pages 164–177. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Munilla:2007:HMF

[MP07] J. Munilla and A. Peinado. HB-MP: a further step in the HB-family of lightweight authentication protocols. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(9):2262–2267, June 20, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Micciancio:2008:OCC

[MP08] Daniele Micciancio and Saurabh Panjwani. Optimal communication complexity of generic multicast key distribution. *IEEE/ACM Transactions on Networking*, 16(4):803–813, August 2008. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Mislove:2006:EBO

[MPHD06] Alan Mislove, Ansley Post, Andreas Haeberlen, and Peter Druschel. Experiences in building and operating ePOST, a reliable peer-to-peer application. *Operating Systems Review*, 40(4):147–159, October 2006. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Moralis:2009:KSA

[MPPM09] Athanasios Moralis, Vassiliki Pouli, Symeon Papavassiliou, and Vasilis Maglaris. A Kerberos security architecture for Web services based instrumentation grids. *Future Generation Computer Systems*, 25(7):804–818, July 2009. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

MacKenzie:2000:PAK

[MPS00] Philip MacKenzie, Sarvar Patel, and Ram Swaminathan. Password-authenticated key exchange based on RSA. *Lecture Notes in Computer Science*, 1976: 599–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760599.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760599.pdf.

Micali:2005:OEC

[MPSW05] Silvio Micali, Chris Peikert, Madhu Sudan, and David A. Wilson. Optimal error correction against computationally bounded noise. In Kilian [Kil05], pages 1–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Monrose:2000:KDB

[MR00] Fabian Monrose and Aviel D. Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4):351–359, February 2000. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.elsevier.com/gej-ng/10/19/19/41/27/30/abstract.html.

MacKenzie:2001:TPG

[MR01a] Philip MacKenzie and Michael K. Reiter. Two-party generation of DSA signatures. In Kilian [Kil01a], pages 137–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390137.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390137.pdf.

Micali:2001:MRR

[MR01b] Silvio Micali and Leonid Reyzin. Min-round resettable zero-knowledge in the public-key model. *Lecture Notes in Computer Science*, 2045:373–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450373.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450373.pdf.

Micali:2001:SPK

[MR01c] Silvio Micali and Leonid Reyzin. Soundness in the public-key model. In Kilian [Kil01a], pages 542–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390542.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390542.pdf.

Murphy:2002:EASa

[MR02a] S. Murphy and M. J. B. Robshaw. Essential algebraic structure within the AES. Report, Information Security Group, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, UK, 2002. 16 pp. URL http://www.isg.rhul.ac.uk/~mrobshaw/aes-crypto.pdf.

Murphy:2002:EASb

[MR02b] Sean Murphy and Matthew J. B. Robshaw. Essential algebraic structure within the AES. In Yung [Yun02a], pages 1–16. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420001.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420001.pdf; http://www.isg.rhul.ac.uk/~mrobshaw/aes-crypto.pdf.

Matyas:2003:TRU

[MR03] Václav Matyás, Jr. and Zdenek Riha. Toward reliable user authentication through biometrics. *IEEE Security & Privacy*, 1(3):45–49, May/June 2003. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://dlib.computer.org/sp/books/sp2003/pdf/j3045.pdf; http://www.computer.org/security/j3045abs.htm.

Micciancio:2009:LBC

[MR09] Daniele Micciancio and Oded Regev. Lattice-based cryptography. In Bernstein et al. [BBD09], pages 147–192. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Monrose:2002:TSG

[MRL+02] Fabian Monrose, Michael Reiter, Qi Li, Daniel P. Lopresti, and Chilin Shih. Toward speech-generated cryptographic keys on resource-constrained devices. In USENIX [USE02b], pages 283–296. ISBN 1-931971-00-5. LCCN ???? URL `http://www.usenix.org/publications/library/proceedings/sec02/monrose.html`.

Mitchell:2006:PPT

[MRST06] John C. Mitchell, Ajith Ramanathan, Andre Scedrov, and Vanessa Teague. A probabilistic polynomial-time process calculus for the analysis of cryptographic protocols. *Theoretical Computer Science*, 353(1–3): 118–164, March 14, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Moghadam:2010:DRN

[MRT10] I. Zarei Moghadam, A. S. Rostami, and M. R. Tanhatalab. Designing a random number generator with novel parallel LFSR substructure for key stream ciphers. In *2010 International Conference on Computer Design and Applications (ICCDA)*, volume 5, pages V5–598–V5–601. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5541188`.

Mayer-Sommer:2001:SAS

[MS01] Rita Mayer-Sommer. Smartly analyzing the simplicity and the power of simple power analysis on smartcards. *Lecture Notes in Computer Science*, 1965:78–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650078.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1965/19650078.pdf`.

Maggi:2002:USV

[MS02a] Paolo Maggi and Riccardo Sisto. Using SPIN to verify security properties of cryptographic protocols. *Lecture Notes in Computer Science*, 2318:187–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http:`

//link.springer-ny.com/link/service/series/0558/bibs/2318/23180187.htm; http://link.springer-ny.com/link/service/series/0558/papers/2318/23180187.pdf.

Maitra:2002:CSB

[MS02b] Subhamoy Maitra and Palash Sarkar. Cryptographically significant Boolean functions with five valued Walsh spectra. *Theoretical Computer Science*, 276(1–2):133–146, April 6, 2002. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/gej-ng/10/41/16/247/27/33/abstract.html.

Menezes:2002:PCI

[MS02c] A. J. (Alfred J.) Menezes and Palash Sarkar, editors. *Progress in cryptology: INDOCRYPT 2002: Third International Conference on Cryptology in India, Hyderabad, India, December 16–18, 2002: Proceedings*, volume 2551 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-00263-4 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I5535 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2551.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2551. Also available via the World Wide Web.

Mitnick:2002:ADC

[MS02d] Kevin D. (Kevin David) Mitnick and William L. Simon. *The art of deception: controlling the human element of security*. John Wiley and Sons, Inc., New York, NY, USA, 2002. ISBN 0-471-23712-4, 0-7645-4280-X (paperback). xvi + 352 pp. LCCN QA76.9.A25 M585 2002. URL http://www.loc.gov/catdir/bios/wiley043/2002512977.html; http://www.loc.gov/catdir/description/wiley036/2002512977.html; http://www.loc.gov/catdir/toc/wiley031/2002512977.html.

Muthukrishnan:2002:IAS

[MS02e] S. Muthukrishnan and S. Cenk Sahinalp. An improved algorithm for sequence comparison with block reversals. *Lecture Notes in Computer Science*, 2286:319–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2286/22860319.htm;

http://link.springer-ny.com/link/service/series/0558/papers/2286/22860319.pdf.

Markowitch:2003:CWV

[MS03a] Olivier Markowitch and Shahrokh Saeednia. Cryptanalysis of the Wu–Varadhrajan fair exchange protocol. *Information Processing Letters*, 87(3):169–171, August 16, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Miklau:2003:CAP

[MS03b] Gerome Miklau and Dan Suciu. Controlling access to published data using cryptography. In Freytag et al. [FLA+03], pages 898–909. ISBN 0-12-722442-4. LCCN ???? URL http://www.vldb.org/dblp/db/indices/a-tree/m/Miklau:Gerome.html.

Martin:2005:PET

[MS05a] David Martin and Andrei Serjantov, editors. *Privacy Enhancing Technologies: 4th International Workshop, PET 2004, Toronto, Canada, May 26–28, 2004. Revised Selected Papers*, volume 3424 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-26203-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 P49 2004.

Meadows:2005:CPA

[MS05b] Catherine Meadows and Paul Syverson, editors. *CCS '05: proceedings of the 12th ACM Conference on Computer and Communications Security: November 7–11, 2005, Alexandria, Virginia, USA*. ACM Press, New York, NY 10036, USA, 2005. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Mahdian:2009:UNI

[MS09a] Babak Mahdian and Stanislav Saic. Using noise inconsistencies for blind image forensics. *Image and Vision Computing*, 27(10): 1497–1503, 2009. CODEN IVCODK. ISSN 0262-8856. URL http://www.sciencedirect.com/science/article/pii/S0262885609000146. Special Section: Computer Vision Methods for Ambient Intelligence.

Manulis:2009:SMF

[MS09b] Mark Manulis and Jörg Schwenk. Security model and framework for information aggregation in sensor networks. *ACM Transactions on Sensor Networks*, 5 (2):13:1–13:??, March 2009. CODEN ???? ISSN

1550-4859 (print), 1550-4867 (electronic).

Mashatan:2009:ITC

[MS09c] Atefeh Mashatan and Douglas R. Stinson. Interactive two-channel message authentication based on Interactive–Collision Resistant hash functions. *International Journal of Information Security*, 8(1):49–60, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0063-0.

Myers:2009:BEC

[MS09d] S. Myers and A. Shelat. Bit encryption is complete. In IEEE [IEE09b], pages 607–616. ISBN 0-7695-3850-9. LCCN QA76 .S95 2009. IEEE Computer Society order number P3850.

Shen:2005:NIW

[mSgFtL05] Rui min Shen, Yong gang Fu, and Hong tao Lu. A novel image watermarking scheme based on support vector regression. *The Journal of Systems and Software*, 78(1):1–8, October 2005. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Marton:2010:RDC

[MSI10] Kinga Marton, Alin Suciu, and Iosif Ignat. Randomness in digital cryptography: a survey. *Romanian Journal of Information Science and Technology*, 13(3):219–240, ???? 2010. CODEN ???? ISSN 1453-8245. URL http:www.imt.ro/romjist/Volum13/Number13_3/pdf/KMarton.pdf.

MacKenzie:2002:TPA

[MSJ02] Philip MacKenzie, Thomas Shrimpton, and Markus Jakobsson. Threshold password-authenticated key exchange: (extended abstract). In Yung [Yun02a], pages 385–400. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/bibs/2455/24550224.htm; http://link.springer-ny.com/link/service/series/0558/papers/2455/24550224.pdf; http://link.springer.de/link/service/series/0558/bibs/2442/24420385.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420385.pdf.

McClure:2003:HEN

[MSK03] Stuart McClure, Joel Scambray, and George Kurtz. *Hacking exposed: network security secrets and solu-*

tions. Osborne/McGraw-Hill, Berkeley, CA, USA, fourth edition, 2003. ISBN 0-07-222742-7. xxiv + 737 pp. LCCN TK5105359 .M48 2003. URL ftp://uiarchive.cso.uiuc.edu/pub/etext/gutenberg/; http://www.loc.gov/catdir/bios/mh051/2004351501.html; http://www.loc.gov/catdir/description/mh051/2004351501.html; http://www.loc.gov/catdir/toc/mh051/2004351501.html.

Matsumoto:2007:FSC

[MSNH07] Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita. A fast stream cipher with huge state space and quasigroup filter for software. In Adams et al. [AMW07], pages 246–263. ISBN 3-540-77360-6. LCCN ????

Miltchev:2008:DAC

[MSP+08] Stefan Miltchev, Jonathan M. Smith, Vassilis Prevelakis, Angelos Keromytis, and Sotiris Ioannidis. Decentralized access control in distributed file systems. *ACM Computing Surveys*, 40(3): 10:1–10:30, August 2008. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Mouratidis:2009:PMD

[MSP09] Kyriakos Mouratidis, Dimitris Sacharidis, and Hweehwa Pang. Partially materialized digest scheme: an efficient verification method for outsourced databases. *VLDB Journal: Very Large Data Bases*, 18(1):363–381, January 2009. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Moran:2004:NIT

[MSTS04] Tal Moran, Ronen Shaltiel, and Amnon Ta-Shma. Non-interactive timestamping in the bounded storage model. In Franklin [Fra04], pages 460–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Myasnikov:2005:PAB

[MSU05] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. A practical attack on a braid group based cryptographic protocol. In Shoup [Sho05a], pages 86–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http:/

/www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Muzereau:2004:EBD

[MSV04] A. Muzereau, N. P. Smart, and F. Vercauteren. The equivalence between the DHP and DLP for elliptic curves used in practical applications. *LMS Journal of Computation and Mathematics*, 7:50–??, 2004. CODEN ???? ISSN 1461-1570.

Marsaglia:2002:SDP

[MT02] George Marsaglia and Wai Wan Tsang. Some difficult-to-pass tests of randomness. *Journal of Statistical Software*, 7(3):1–8, 2002. CODEN JSSOBK. ISSN ???? URL http://www.jstatsoft.org/v07/i03; http://www.jstatsoft.org/v07/i03/tuftests.c; http://www.jstatsoft.org/v07/i03/tuftests.pdf; http://www.jstatsoft.org/v07/i03/updates.

Meseguer:2007:SRA

[MT07] José Meseguer and Prasanna Thati. Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols. *Higher-Order and Symbolic Computation*, 20(1–2):123–160, June 2007. CODEN LSCOEX. ISSN 1388-3690 (print), 2212-0793 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1388-3690&volume=20&issue=1&spage=123.

Ma:2009:NAS

[MT09] Di Ma and Gene Tsudik. A new approach to secure logging. *ACM Transactions on Storage*, 5(1):2:1–2:??, March 2009. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Muller:2001:SWB

[Mül01a] Siguna Müller. On the security of a Williams based public key encryption scheme. In *Public key cryptography (Cheju Island, 2001)*, volume 1992 of *Lecture Notes in Comput. Sci.*, pages 1–18. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920001.pdf.

Muller:2001:SIC

[Mül01b] Siguna Müller. A survey of IND-CCA secure public-key encryption schemes relative to factoring. In *Public-key cryptography and computational number theory (War-*

saw, 2000)*, pages 181–196. Walter de Gruyter, New York, NY, USA, 2001.

Mullins:2002:MUC

[Mul02] J. Mullins. Making unbreakable code. *IEEE Spectrum*, 39(5):40–45, May 2002. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Mullins:2006:CC

[Mul06] J. Mullins. Chaotic communication. *IEEE Spectrum*, 43(1):11–12, January 2006. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Munro:2008:DE

[Mun08] Ken Munro. Desktop encryption. *Network Security*, 2008(12):4–6, December 2008. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485808701387.

Murphy:2000:KST

[Mur00] S. Murphy. The key separation of Twofish. Comments on AES round 2 submitted to NIST., March 2000.

Murray:2001:CDC

[Mur01] Eric Murray. Changes in deployment of cryptography, and possible causes, 2001. URL http://www.usenix.org/publications/library/proceedings/sec01/murray/index.htm. Unpublished invited talk, Tenth USENIX Security Symposium, August 13–17, 2001, Washington, DC, USA.

Murray:2002:IYP

[Mur02] Mark R. V. Murray. An implementation of the Yarrow PRNG for FreeBSD. In USENIX [USE02a], pages 47–53. ISBN 1-880446-02-2. LCCN QA76.76.O63 B736 2002. URL http://www.usenix.org/publications/library/proceedings/bsdcon02/murray.html.

Murton:2006:CGH

[Mur06] Daniel Murton. Crypto goes to the heart. *Network Security*, 2006(5):19, May 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485806703907.

Moriai:2000:PTL

[MV00] Shiho Moriai and Serge Vaudenay. On the pseudorandomness of top-level schemes of block ciphers. *Lecture Notes in Computer Science*, 1976:289–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760289.

htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760289.pdf.

Meister:2001:PPG

[MV01] Gisela Meister and Michael Vogel. Protection profiles and generic security targets for smart cards as secure signature creation devices — existing solutions for the payment sector. *Lecture Notes in Computer Science*, 2140:179–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400179.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400179.pdf.

Micciancio:2003:SZK

[MV03a] Daniele Micciancio and Salil P. Vadhan. Statistical zero-knowledge proofs with efficient provers: Lattice problems and more. In Boneh [Bon03], pages 282–298. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Morrow:2003:DIB

[MV03b] Monique Morrow and Kateel Vijayananda. *Developing IP-based services: solutions for service providers and vendors*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 2003. ISBN 1-55860-779-X. xxi + 313 pp. LCCN TK5105.5 .M72 2003. US$49.95.

Micciancio:2004:CTA

[MW04] Daniele Micciancio and Bogdan Warinschi. Completeness theorems for the Abadi–Rogaway language of encrypted expressions. *Journal of Computer Security*, 12(1):99–129, ???? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ma:2006:ADS

[MW06] Mingchao Ma and Steve Woodhead. Authentication delegation for subscription-based remote network services. *Computers & Security*, 25(5):371–378, July 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404806000575.

Morelli:2001:JAH

[MWM01] Ralph Morelli, Ralph Walde, and Gregg Marcuccio. A Java API for historical ciphers: an object-oriented design project. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 33(1): 307–311, March 2001. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Malan:2008:IPK

[MWS08] David J. Malan, Matt Welsh, and Michael D. Smith. Implementing public-key infrastructure for sensor networks. *ACM Transactions on Sensor Networks*, 4(4):22:1–22:??, August 2008. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

MRaihi:2001:CAS

[MY01] David M'Raïhi and Moti Yung. E-commerce applications of smart cards. *Computer Networks (Amsterdam, Netherlands: 1999)*, 36(4):453–472, July 16, 2001. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.elsevier.nl/gej-ng/10/15/22/61/28/31/abstract.html; http://www.elsevier.nl/gej-ng/10/15/22/61/28/31/article.pdf.

McCook:2001:NSS

[MYC01] Alison McCook, Philip Yam, and Graham P. Collins. News scan: The not so sheltering sky; computer: Hack job; tissue engineering: Fat into cartilage; psychology: Holier than thou; astronomy: Otherworldly ocean; physics: Microscopic maelstrom; medicine: Fetal cell setback. *Scientific American*, 284(5):24–25, May 2001. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/2001/0501issue/0501inbrief.html.

Morelos-Zaragoza:2002:AEC

[MZ02] Robert Morelos-Zaragoza. *The Art of Error Correcting Coding*. John Wiley and Sons, Inc., New York, NY, USA, 2002. ISBN 0-471-49581-6. xvi + 221 pp. LCCN ???? UK£45.00, US$95.00. URL http://www.loc.gov/catdir/description/wiley035/2002280749.html; http://www.loc.gov/catdir/toc/wiley023/2002280749.html.

Matsui:2004:SAC

[MZ04] Mitsuru Matsui and Robert Zuccherato, editors. *Selected Areas in Cryptography: 10th Annual International Workshop, SAC 2003, Ottawa, Canada, August 14–15, 2003, Revised Papers*, volume 3006 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-21370-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://link.springer-ny.com/link/service/series/0558/tocs/t3006.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3006; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b96837.

Nagy:2007:AQK

[NA07] Naya Nagy and Selim G. Akl. Authenticated quantum key distribution without classical communication. *Parallel Processing Letters*, 17(3):323–335, September 2007. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Naik:2003:DSW

[NABG03] Vinayak Naik, Anish Arora, Sandip Bapat, and Mohamed Gouda. Dependable systems: Whisper: Local secret maintenance in sensor networks. *IEEE Distributed Systems Online*, 4(9), 2003. CODEN ???? ISSN 1541-4922 (print), 1558-1683 (electronic). URL http://dsonline.computer.org/0309/f/gaep.htm.

Naccache:2001:TCC

[Nac01] David Naccache, editor. *Topics in cryptology, CT-RSA 2001: the Cryptographers' Track at RSA Conference 2001, San Francisco, CA, USA, April 8–12, 2001: Proceedings*, volume 2020 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-41898-9 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.2020; QA76.9.A25 R753 2001. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2020.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2020.

Naftali:2005:BSS

[Naf05] Timothy J. Naftali. *Blind spot: the secret history of American counterterrorism*. Basic Books, New York, NY, USA, 2005. ISBN 0-465-09281-0 (hardcover). xv + 399 pp. LCCN HV6432 .N34 2005. URL http://www.loc.gov/catdir/toc/ecip057/2005003248.html.

Nakai:2001:SFW

[Nak01] Yuichi Nakai. Semi fragile watermarking based on wavelet transform. *Lecture Notes in Computer Science*, 2195:796–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950796.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950796.pdf.

Namprempre:2002:SCB

[Nam02] Chanathip Namprempre. Secure channels based on authenticated encryption schemes: a simple characterization. *Lecture Notes in Computer Science*, 2501:515–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010515.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010515.pdf.

Naor:2002:DRA

[Nao02] Moni Naor. Deniable ring authentication. In Yung [Yun02a], pages 481–498. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420210.htm; http://link.springer.de/link/service/series/0558/bibs/2442/24420481.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420210.pdf; http://link.springer.de/link/service/series/0558/papers/2442/24420481.pdf.

Naor:2003:CAC

[Nao03] Moni Naor. On cryptographic assumptions and challenges. In Boneh [Bon03], pages 96–109. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Naor:2004:TCF

[Nao04] Moni Naor, editor. *Theory of Cryptography: First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19–21, 2004: Proceed-*

ings, volume 2951 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-21000-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C6676 2004. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2951.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2951; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b95566.

NIST:2000:FPD

[Nat00] National Institute of Standards and Technology. *FIPS PUB 186-2: Digital Signature Standard (DSS)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 27, 2000. URL http://www.itl.nist.gov/fipspubs/fip186-2.pdf.

Nazario:2002:RYS

[Naz02] Jose Nazario. A rough year for SSH. *Linux Journal*, 95: ??, March 2002. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://noframes.linuxjournal.com/lj-issues/issue95/article.php?sid=5672. Web only.

Nieto:2001:PKC

[NBD01] Juan Manuel González Nieto, Colin Boyd, and Ed Dawson. A public key cryptosystem based on the subgroup membership problem. *Lecture Notes in Computer Science*, 2229: 352–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290352.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290352.pdf.

Nghiem:2009:FBI

[NC09] Thao P. Nghiem and Tae Ho Cho. A fuzzy-based interleaved multi-hop authentication scheme in wireless sensor networks. *Journal of Parallel and Distributed Computing*, 69(5):441–450, May 2009. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Ning:2004:TTA

[NCRX04] Peng Ning, Yun Cui, Douglas S. Reeves, and Dingbang Xu. Techniques and tools for analyzing intrusion alerts. *ACM Transactions on Information and*

System Security, 7(2):274–318, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Nedjah:2005:SHC

[Nd05] N. Nedjah and L. de, Macedo, Mourelle. Software/hardware co-design of efficient and secure cryptographic hardware. *J.UCS: Journal of Universal Computer Science*, 11(1):66–??, January 28, 2005. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_11_1/software_hardware_co_design.

Nash:2001:PIM

[NDJB01] Andrew Nash, William Duane, Celia Joseph, and Derek Brink. *PKI: Implementing and Managing E-Security*. McGraw-Hill, New York, NY, USA, 2001. ISBN 0-07-213123-3. xxii + 513 pp. LCCN QA76.9.A25 P5 2001. US$49.99.

Nedjah:2004:ECH

[NdM04] Nadia Nedjah and Luiza de Macedo Mourelle, editors. *Embedded cryptographic hardware: methodologies and architectures*. Nova Science Publishers, New York, NY, USA, 2004. ISBN 1-59454-012-8 (hardcover). ix + 295 pp. LCCN TK5102.94 .E49 2004. URL http://www.loc.gov/catdir/toc/ecip0417/2004008204.html.

Nedjah:2006:NTC

[NdM06] Nadia Nedjah and Luiza de Macedo Mourelle, editors. *New trends in cryptographic systems*. Nova Science Publishers, Hauppauge, NY, USA, 2006. ISBN 1-59454-977-X. ???? pp. LCCN TK7895.E42 N42 2006. URL http://www.loc.gov/catdir/toc/ecip066/2006001583.html.

Netscape:2004:HSW

[Net04] Netscape Communications, Inc. How SSL works. World-wide Web document., August 27, 2004. URL http://developer.netscape.com/tech/security/ssl/howitworks.html; http://web.archive.org/web/20040827080204/. This is a tutorial of how the Secure Sockets Layer (SSL) protocol works.

Neuenschwander:2004:PSM

[Neu04] Daniel Neuenschwander. *Probabilistic and Statistical Methods in Cryptology: An Introduction by Selected Topics*, volume 3028 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22001-1. ISSN 0302-9743 (print), 1611-3349 (electronic). x + 158 pp. LCCN QA76 A1 L43 3028. URL http://link.springer-ny.com/link/service/series/0558/tocs/t3028.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3028; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b97045.

Neuenschwander:2006:IMM

[Neu06] Mike Neuenschwander. Identity management market shifts — who's out there? *Network Security*, 2006(12): 7–10, December 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485806704615.

Neve:2003:STF

[NFQ03] Amaury Nève, Denis Flandre, and Jean-Jacques Quisquater. SOI technology for future high-performance smart cards. *IEEE Micro*, 23(3):58–67, May/June 2003. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://csdl.computer.org/comp/mags/mi/2003/03/m3058abs.htm; http://csdl.computer.org/dl/mags/mi/2003/03/m3058.pdf.

Nguyen:2001:TFLb

[Ngu01] Phong Q. Nguyen. The two faces of lattices in cryptology. *Lecture Notes in Computer Science*, 2259: 313–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2259/22590313.htm; http://link.springer-ny.com/link/service/series/0558/papers/2259/22590313.pdf.

Nguyen:2005:RBP

[Ngu05] Minh-Huyen Nguyen. The relationship between password-authenticated key exchange and other cryptographic primitives. In Kilian [Kil05], pages 457–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Nordholt:2002:NFC

[NH02] Jane E. Nordholt and Richard J. Hughes. A new face for cryptography. *Los Alamos Science*, 27:68–85, 2002. CO-

DEN LASCDI. ISSN 0273-7116. URL http://library.lanl.gov/cgi-bin/getfile?27-08.pdf.

Nyberg:2003:SAC

[NH03] Kaisa Nyberg and Howard Heys, editors. *Selected areas in cryptography: 9th annual International Workshop, SAC 2002, St. John's, Newfoundland, Canada, August 15–16, 2002: Revised Papers*, volume 2595 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-00622-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 S22 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2595.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2595. Also available via the World Wide Web.

Nicholson:2001:YBC

[Nic01] John Nicholson. You've been cracked … and now you're sued. *;login: the USENIX Association newsletter*, 26(2):??, April 2001. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/2001-04/pdfs/nicholson.pdf.

Niederreiter:2002:BRC

[Nie02a] Harald Niederreiter. Book review: *Cryptography and computational number theory*. *Mathematics of Computation*, 71(239):??, July 2002. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2002-71-239/S0025-5718-02-01454-0/bookrev-S0025-5718-02-01454-0.html; http://www.ams.org/mcom/2002-71-239/S0025-5718-02-01454-0/S0025-5718-02-01454-0.dvi; http://www.ams.org/mcom/2002-71-239/S0025-5718-02-01454-0/S0025-5718-02-01454-0.pdf; http://www.ams.org/mcom/2002-71-239/S0025-5718-02-01454-0/S0025-5718-02-01454-0.ps; http://www.ams.org/mcom/2002-71-239/S0025-5718-02-01454-0/S0025-5718-02-01454-0.tex.

Nielsen:2002:SRO

[Nie02b] Jesper Buus Nielsen. Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case. In Yung [Yun02a], pages 111–126. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN

QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420111.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420111.pdf.

Nielsen:2002:TPF

[Nie02c] Jesper Buus Nielsen. A threshold pseudorandom function construction and its applications. In Yung [Yun02a], pages 401–416. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Nievergelt:2002:FLM

[Nie02d] Yves Nievergelt. *Foundations of Logic and Mathematics: Applications to Computer Science and Cryptography*. Birkhäuser Verlag, Basel, Switzerland, 2002. ISBN 0-8176-4249-8 , 3-7643-4249-8. xvi + 415 pp. LCCN QA9 .N53 2002. URL http://www.loc.gov/catdir/enhancements/fy0812/2001052551-d.html; http://www.loc.gov/catdir/enhancements/fy0812/2001052551-t.html.

Niederreiter:2004:BRC

[Nie04] H. Niederreiter. Book review: *Cryptographic applications of analytic number theory*. *Mathematics of Computation*, 73(247):1581–1582, July 2004. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/home.html; http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/S0025-5718-04-01695-3.dvi; http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/S0025-5718-04-01695-3.pdf; http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/S0025-5718-04-01695-3.ps; http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/S0025-5718-04-01695-3.tex.

Nikander:2002:DSAa

[Nik02a] Pekka Nikander. Denial-of-service, address ownership, and early authentication in the IPv6 world. *Lecture Notes in Computer Science*, 2467:12–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2467/24670012.htm; http://link.springer.de/link/

service/series/0558/papers/2467/24670012.pdf.

Nikander:2002:DSAb

[Nik02b] Pekka Nikander. Denial of service, address ownership, and early authentication in the IPv6 world (transcript of discussion). *Lecture Notes in Computer Science*, 2467:22–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2467/24670022.htm; http://link.springer.de/link/service/series/0558/papers/2467/24670022.pdf.

NIST:2000:TAE

[NIS00] NIST, editor. *The Third Advanced Encryption Standard Candidate Conference, April 13–14, 2000, New York, NY, USA*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2000. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

NIST:2001:CT

[NIS01a] NIST. Cryptographic toolkit. World-Wide Web document, 2001. URL http://csrc.nist.gov/CryptoToolkit/.

NIST:2001:SRC

[NIS01b] NIST. Security requirements for cryptographic modules. Federal Information Processing Standards Publication FIPS PUB 140-2, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, May 25, 2001.

Nisley:2003:ELH

[Nis03a] E. Nisley. Ed looks at the history of cryptography and examines what it means for embedded systems developers programming in Java today. *Dr. Dobb's Journal of Software Tools*, 28 (11):73–75, 2003. CODEN DDJOEB. ISSN 1044-789X.

NIST:2003:RKE

[NIS03b] NIST. Recommendation on key establishment schemes. NIST Special Publication 800-56, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 2003.

URL http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf.

Nitaj:2009:CRCo

[Nit09] Abderrahmane Nitaj. Cryptanalysis of RSA with constrained keys. *International Journal of Number Theory (IJNT)*, 5(2):311–325, March 2009. ISSN 1793-0421 (print), 1793-7310 (electronic). URL https://www.worldscientific.com/doi/10.1142/S1793042109002122.

Nagaj:2006:OQE

[NK06] Daniel Nagaj and Iordanis Kerenidis. On the optimality of quantum encryption schemes. *Journal of Mathematical Physics*, 47 (9):092102, September 2006. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL http://jmp.aip.org/resource/1/jmapaq/v47/i9/p092102_s1.

Ning:2008:MAA

[NLD08] Peng Ning, An Liu, and Wenliang Du. Mitigating DoS attacks against broadcast authentication in wireless sensor networks. *ACM Transactions on Sensor Networks*, 4(1):1:1–1:??, January 2008. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Nigrini:2009:DDU

[NM09] Mark J. Nigrini and Steven J. Miller. Data diagnostics using second-order tests of Benford's Law. *Auditing: A Journal of Practice & Theory*, 28(2):305–324, November 2009. CODEN ???? ISSN 0278-0380 (print), 1558-7991 (electronic). URL http://aaapubs.org/loi/ajpt; http://link.aip.org/link/AJPTXX/v28/i2/p305/s1.

Nagao:2005:UCS

[NMO05] Waka Nagao, Yoshifumi Manabe, and Tatsuaki Okamoto. A universally composable secure channel based on the KEM–DEM framework. In Kilian [Kil05], pages 426–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Nozaki:2001:IRA

[NMSK01] H. Nozaki, M. Motoyama, A. Shimbo, and S. Kawamura. Implementation of RSA algorithm based on RNS Montgomery multiplication. *Lecture Notes in Computer Science*, 2162: 364–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620364.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620364.pdf`.

Northcutt:2002:NID

[NN02] Stephen Northcutt and Judy Novak. *Network intrusion detection*. New Riders Publishing, Carmel, IN, USA, third edition, 2002. ISBN 0-7357-1265-4. xvii + 490 pp. LCCN TK5105.59 .N475 2003.

Naor:2003:CFP

[NN03] Dalit Naor and Moni Naor. Cover feature: Protecting cryptographic keys: the trace-and-revoke approach. *Computer*, 36(7): 47–53, July 2003. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://csdl.computer.org/dl/mags/co/2003/07/r7047.htm; http://csdl.computer.org/dl/mags/co/2003/07/r7047.pdf; http://www.computer.org/computer/co2003/r7047abs.htm`.

Nikov:2006:RBV

[NN06] Ventzislav Nikov and Svetla Nikova. On a relation between verifiable secret sharing schemes and a class of error-correcting codes. In Ytrehus [Ytr06], pages 275–290. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Navin:2010:ETU

[NNAM10] A. H. Navin, Z. Navadad, B. Aasadi, and M. Mirnia. Encrypted tag by using data-oriented random number generator to increase security in wireless sensor network. In *2010 International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 335–338. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5701989`.

Naor:2001:RTS

[NNL01] Dalit Naor, Moni Naor, and Jeff Lotspiech. Revocation and tracing schemes for stateless receivers. In Kilian [Kil01a], pages 41–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390041.htm; http://link.springer-`

ny.com/link/service/series/0558/papers/2139/21390041.pdf.

Naor:2005:ECH

[NNT05] Moni Naor, Asaf Nussboim, and Eran Tromer. Efficiently constructible huge graphs that preserve first order properties of random graphs. In Kilian [Kil05], pages 66–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Novak:2001:SBA

[Nov01] Roman Novak. SPA-based adaptive chosen-ciphertext attack on RSA implementation. *Lecture Notes in Computer Science*, 2274: 252–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740252.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740252.pdf.

Naccache:2002:PKC

[NP02a] David Naccache and Pascal Paillier, editors. *Public key cryptography: 4th [i.e., 5th] International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002, Paris, France, February 12–14, 2002: Proceedings*, volume 2274 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-43168-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I567 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2274.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2274.

Nguyen:2002:AIN

[NP02b] Phong Q. Nguyen and David Pointcheval. Analysis and improvements of NTRU encryption paddings. In Yung [Yun02a], pages 210–225. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420210.htm; http:

//link.springer.de/link/service/series/0558/papers/2442/24420210.pdf.

Nichols:2007:MFD

[NP07] Elizabeth A. Nichols and Gunnar Peterson. A metrics framework to drive application security improvement. *IEEE Security & Privacy*, 5(2):88–91, March/April 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Nakahara:2001:LCR

[NPV01] Jorge Nakahara, Jr., Bart Preneel, and Joos Vandewalle. Linear cryptanalysis of reduced-round versions of the SAFER block cipher family. *Lecture Notes in Computer Science*, 1978:244–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780244.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780244.pdf.

Naor:2004:NTC

[NR04] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *Journal of the ACM*, 51(2):231–262, March 2004. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Nichols:2000:DYD

[NRR00] Randall K. Nichols, Daniel J. Ryan, and Julie J. C. H. Ryan. *Defending your digital assets: against hackers, crackers, spies and thieves*. McGraw-Hill, New York, NY, USA, 2000. ISBN 0-07-212285-4. xxxv + 858 pp. LCCN QA76.9.A25 N528 2000. US$59.99. URL http://corpitk.earthweb.com/reference/0072122854.html.

Neraud:2001:CFD

[NS01a] Jean Néraud and Carla Selmi. On codes with a finite deciphering delay: constructing uncompletable words. *Theoretical Computer Science*, 255(1–2):151–162, March 28, 2001. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.nl../28/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/197/21/28/article.pdf.

Nguyen:2001:ISA

[NS01b] Phong Q. Nguyen and Igor E. Shparlinski. On the insecurity of a server-aided RSA protocol. *Lecture Notes in Computer Science*, 2248:21–??, 2001. CODEN LNCSD9. ISSN 0302-

9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480021.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480021.pdf.

Nguyen:2001:TFLa

[NS01c] Phong Q. Nguyen and Jacques Stern. The two faces of lattices in cryptology. *Lecture Notes in Computer Science*, 2146: 146–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2146/21460146.htm; http://link.springer-ny.com/link/service/series/0558/papers/2146/21460146.pdf.

Narayanan:2005:FDA

[NS05a] Arvind Narayanan and Vitaly Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In Meadows and Syverson [MS05b], pages 364–372. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Narayanan:2005:ODG

[NS05b] Arvind Narayanan and Vitaly Shmatikov. Obfuscated databases and group privacy. In Meadows and Syverson [MS05b], pages 102–111. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Nguyen:2005:FPL

[NS05c] P. Nguyen and D. Stehle. Floating-point LLL revisited. *Lecture Notes in Computer Science*, 3494: 215–233, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:2005:PSE

[NSNK05] L. Nguyen, R. Safavi-Naini, and K. Kurosawa. A provably secure and efficient verifiable shuffle based on a variant of the Paillier cryptosystem. *J.UCS: Journal of Universal Computer Science*, 11(6):986–1010, ???? 2005. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_11_6/a_provably_secure_and.

Nishioka:2002:DAF

[NSS02] Mototsugu Nishioka, Hisayoshi Satoh, and Kouichi Sakurai. Design and analysis of fast provably secure public-key cryptosystems based on a modular squaring. *Lecture Notes in Computer Science*, 2288:81–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/

link/service/series/0558/bibs/2288/22880081.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880081.pdf.

Nahum:2007:ESS

[NTW07] Erich M. Nahum, John Tracey, and Charles P. Wright. Evaluating SIP server performance. *ACM SIGMETRICS Performance Evaluation Review*, 35(1): 349–350, June 2007. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Nyberg:2001:CTC

[Nyb01] Kaisa Nyberg. Correlation theorems in cryptanalysis. *Discrete Applied Mathematics*, 111(1-2):177–188, 2001. CODEN DAMADU. ISSN 0166-218X (print), 1872-6771 (electronic).

Nenadic:2005:RBC

[NZCG05] A. Nenadic, N. Zhang, B. Cheetham, and C. Goble. RSA-based certified delivery of E-goods using verifiable and recoverable signature encryption. *J.UCS: Journal of Universal Computer Science*, 11(1):175–192, January 28, 2005. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_11_1/rsa_based_certified_delivery.

Nenadic:2005:RBV

[NZS05] Aleksandra Nenadić, Ning Zhang, and Qi Shi. RSA-based Verifiable and Recoverable Encryption of Signatures and its application in certified e-mail delivery. *Journal of Computer Security*, 13(5):757–777, ???? 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Olson:2003:QHK

[OC03] Lynne Olson and Stanley Cloud. *A question of honor: the Kościuszko Squadron: forgotten heroes of World War II*. Knopf, New York, NY, USA, 2003. ISBN 0-375-41197-6. xii + 495 pp. LCCN D786 .O57 2003. URL http://www.loc.gov/catdir/bios/random051/2002044826.html; http://www.loc.gov/catdir/description/random0414/2002044826.html; http://www.loc.gov/catdir/samples/random045/2002044826.html.

Oechslin:2003:MFC

[Oec03] Philippe Oechslin. Making a faster cryptanalytic time-memory trade-off. In Boneh [Bon03], pages 617–630. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/

link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Oppliger:2008:STSb

[OHB08a] Rolf Oppliger, Ralf Hauser, and David Basin. SSL/TLS session-aware user authentication. *Computer*, 41(3):59–65, March 2008. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Oppliger:2008:STSa

[OHB08b] Rolf Oppliger, Ralf Hauser, and David Basin. SSL/TLS session-aware user authentication revisited. *Computers & Security*, 27(3–4):64–70, May/June 2008. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808000102.

Oiwa:2009:IMS

[Oiw09] Yutaka Oiwa. Implementation of the memory-safe full ANSI-C compiler. *ACM SIGPLAN Notices*, 44(6):259–269, June 2009. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Okamoto:2000:ACA

[Oka00] Tatsuaki Okamoto, editor. *Advances in cryptology — ASIACRYPT 2000: 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3–7, 2000: proceedings*, volume 1976 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-41404-5 (softcover). LCCN QA76.9.A25 I555 2000.

Okamoto:2004:TCC

[Oka04] Tatsuaki Okamoto, editor. *Topics in Cryptology—CT-RSA 2004: The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23–27, 2004: Proceedings*, volume 2964 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-20996-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2004. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2964.htm; http://www.springerlink.com/openurl.asp?genre=issue&

issn=0302-9743&volume=2964; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b95630.

Ohzahata:2002:FAM

[OKE02] Satoshi Ohzahata, Shigetomo Kimura, and Yoshihiko Ebihara. A fast authentication method for secure and seamless handoff. *Lecture Notes in Computer Science*, 2344: 243–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2344/23440243.htm; http://link.springer.de/link/service/series/0558/papers/2344/23440243.pdf.

Ogata:2006:OSS

[OKS06] Wakaha Ogata, Kaoru Kurosawa, and Douglas R. Stinson. Optimum secret sharing scheme secure against cheating. *SIAM Journal on Discrete Mathematics*, 20(1):79–95, January 2006. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Olson:2000:SCT

[Ols00] Adam Olson. Scaring crackers away with TCP wrapper. *Sys Admin: The Journal for UNIX Systems Administrators*, 9(10):67–71, October 2000. CODEN SYADE7. ISSN 1061-2688. URL http://www.samag.com/.

Ohigashi:2009:PMF

[OM09] Toshihiro Ohigashi and Masakatu Morii. A practical message falsification attack on WPA. Technical report, Hiroshima University, 1-4-2 Kagamiyama, Higashi-Hiroshima, 739-8511 Japan, July 15, 2009. URL http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf.

Ohkuma:2001:BCH

[OMSK01] Kenji Ohkuma, Hirofumi Muratani, Fumihiko Sano, and Shinichi Kawamura. The block cipher hierocrypt. *Lecture Notes in Computer Science*, 2012: 72–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120072.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120072.pdf.

Ohbuchi:2002:FDA

[OMT02] Ryutarou Ohbuchi, Akio Mukaiyama, and Shigeo Takahashi. A frequency-domain approach to watermarking 3D shapes. *Computer Graphics Forum*, 21(3): 373–382, September 2002. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Onions:2001:SSI

[Oni01] Paul Onions. On the strength of simply-iterated Feistel ciphers with whitening keys. *Lecture Notes in Computer Science*, 2020: 63–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200063.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200063.pdf.

Ors:2003:PAA

[ÖOP03] Sıddıka Berna Örs, Elisabeth Oswald, and Bart Preneel. Power-analysis attacks on an FPGA — first experimental results. In Walter et al. [WKP03], pages 35–50. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Okamoto:2001:GPN

[OP01a] Tatsuaki Okamoto and David Pointcheval. The gap-problems: a new class of problems for the security of cryptographic schemes. *Lecture Notes in Computer Science*, 1992: 104–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920104.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920104.pdf.

Okamoto:2001:RRE

[OP01b] Tatsuaki Okamoto and David Pointcheval. REACT: rapid enhanced-security asymmetric cryptosystem transform. *Lecture Notes in Computer Science*, 2020:159–175, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Oppliger:2001:SMP

[Opp01] Rolf Oppliger. *Secure messaging with PGP and S/MIME*. Artech House computer security series. Artech House Inc., Norwood, MA, USA, 2001.

ISBN 1-58053-161-X. xxiii + 305 pp. LCCN TK5102.85 .O67 2001. URL http://www.artechhouse.com/Detail.aspx?strIsbn=978-1-58053-161-0.

Oppliger:2005:CC

[Opp05] Rolf Oppliger. *Contemporary cryptography*. Artech House computer security series. Artech House Inc., Norwood, MA, USA, 2005. ISBN 1-58053-642-5. xxv + 503 pp. LCCN Z103 .O66 2005. URL http://www.artechhouse.com/Detail.aspx?strIsbn=978-1-58053-642-4.

Ortiz:2000:ITW

[Ort00] Sixto Ortiz Jr. Industry trends: Will PKI become a key to online security? *Computer*, 33(12): 13–15, December 2000. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co2000/pdf/rz013.pdf.

Okeya:2000:PAB

[OS00] Katsuyuki Okeya and Kouichi Sakurai. Power analysis breaks elliptic curve cryptosystems even secure against the timing attack. *Lecture Notes in Computer Science*, 1977: 178–190, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Okeya:2001:EEC

[OS01] K. Okeya and K. Sakurai. Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve. *Lecture Notes in Computer Science*, 2162: 126–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620126.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620126.pdf.

Ostrovsky:2005:PSS

[OS05] Rafail Ostrovsky and William E. Skeith III. Private searching on streaming data. In Shoup [Sho05a], pages 223–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Oren:2006:PAR

[OS06] Yossi Oren and Adi Shamir.

Power analysis of RFID tags. Technical report, Faculty of Mathematics and Computer Science, Weizmann Institute, POB 26, Rehovot 76100, Israel, 2006. URL `http://www.wisdom.weizmann.ac.il/~yossio/rfid/`.

Obimbo:2007:PAD

[OS07] Charlie Obimbo and Behzad Salami. A parallel algorithm for determining the inverse of a matrix for use in blockcipher encryption/decryption. *The Journal of Supercomputing*, 39(2):113–130, February 2007. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=39&issue=2&spage=113`.

Oury:2008:PP

[OS08] Nicolas Oury and Wouter Swierstra. The power of Pi. *ACM SIGPLAN Notices*, 43(9):39–50, September 2008. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Overbeck:2009:CBC

[OS09] Raphael Overbeck and Nicolas Sendrier. Code-based cryptography. In Bernstein et al. [BBD09], pages 95–146. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Okeya:2004:SBR

[OSSST04] Katsuyuki Okeya, Katja Schmidt-Samoa, Christian Spahn, and Tsuyoshi Takagi. Signed binary representations revisited. In Franklin [Fra04], pages 123–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099`.

Osvik:2005:CAC

[OST05] Dag Arne Osvik, Adi Shamir, and Eran Tromer. Cache attacks and countermeasures: the case of AES: (extended version). Technical report, Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel, October 8, 2005. URL `http://www.wisdom.weizmann.ac.il/~tromer/papers/cache.pdf`.

Osvik:2006:CAC

[OST06] Dag Arne Osvik, Adi Shamir, and Eran Tromer.

Cache attacks and countermeasures: the case of AES. In ????, editor, *Topics in Cryptology — CT-RSA*, pages 1–20. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN ???? LCCN ???? URL ????.

Osvik:2000:SS

[Osv00] Dag Arne Osvik. Speeding up Serpent. In NIST [NIS00], pages 317–329. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Okeya:2003:MFC

[OT03a] Katsuyuki Okeya and Tsuyoshi Takagi. A more flexible countermeasure against side channel attacks using window method. In Walter et al. [WKP03], pages 397–410. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Okeya:2003:WNM

[OT03b] Katsuyuki Okeya and Tsuyoshi Takagi. The width-w NAF method provides small memory and fast elliptic scalar multiplications secure against side channel attacks. In Joye [Joy03b], pages 328–342. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Okada:2001:IEC

[OTIT01] Souichi Okada, Naoya Torii, Kouichi Itoh, and Masahiko Takenaka. Implementation of elliptic curve cryptographic coprocessor over GF(2^m) on an FPGA. *Lecture Notes in Computer Science*, 1965:25–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650025.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650025.pdf.

Okamoto:2000:QPK

[OTU00] Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama. Quantum public-key cryptosystems. In Bellare [Bel00], pages 147–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800147.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800147.pdf.

Ouellette:2005:PPM

[Oue05] John Ouellette. Paranoid penguin: Managing SSH for scripts and `cron` jobs. *Linux Journal*, 2005 (137):13, September 2005. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Overbeck:2006:EGA

[Ove06] Raphael Overbeck. Extending Gibson's attacks on the GPT cryptosystem. In Ytrehus [Ytr06], pages 178–188. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Onieva:2008:MNS

[OZL08] Jose A. Onieva, Jianying Zhou, and Javier Lopez. Multiparty nonrepudiation: a survey. *ACM Computing Surveys*, 41(1):5:1–5:43, December 2008. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Paeng:2003:SCU

[Pae03] Seong-Hun Paeng. On the security of cryptosystem using automorphism groups. *Information Processing Letters*, 88(6):293–298, December 31, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Page:2003:BRW

[Pag03] Sophie Page. Book review: William R. Newman and Anthony Grafton (eds.), Secrets of Nature: Astrology and Alchemy in Early Modern Europe. Transformations: Studies in the History of Science and Technology. Cambridge, MA and London: MIT Press, 2001. Pp. 443. ISBN 0-262-14075-6. £34.50 (hardcover). *British Journal for the History of Science*, 36(1):87–127, March 2003. CODEN BJHSAT. ISSN 0007-0874 (print), 1474-001X (electronic). URL http://www.jstor.org/stable/4028320.

Palmer:2002:TMQ

[Pal02] Chloë Palmer. Toshiba makes quantum crypto breakthrough. *Network Security*, 2002(1):6, January 1, 2002. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485802001150.

Panditaratne:2007:TRN

[Pan07] Vidura Panditaratne. True random number generator goes online. World-Wide Web document, July 18, 2007. URL http://pressesc.com/01184778212_qrbgs; http://qrbg.irb.hr/; http://random.irb.hr/.

Papanikolaou:2005:BRBa

[Pap05] Nikolaos Papanikolaou. Book review: *Data Privacy and Security*, by David Salomon; Spring-Verlag, 2003, $51.48, Hardcover. *ACM SIGACT News*, 36(2):8–13, June 2005. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL http://doi.acm.org/10.1145/1067309.1067315. See [Sal03a].

Park:2004:APP

[Par04] Chang-Seop Park. Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 44(2):267–273, February 5, 2004. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Pass:2003:DCR

[Pas03] Rafael Pass. On deniability in the common reference string and random oracle model. In Boneh [Bon03], pages 316–337. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Pass:2005:UCN

[Pas05] Rafael Pass and abhi shelat. Unconditional characterizations of non-interactive zero-knowledge. In Shoup [Sho05a], pages 118–?? ISBN 3-540-

28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Patterson:2001:DFI

[Pat01] Cameron Patterson. A dynamic FPGA implementation of the Serpent block cipher. *Lecture Notes in Computer Science*, 1965: 141–155, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650141.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650141.pdf.

Patiyoot:2002:MSE

[Pat02a] D. Patiyoot. Migration /evolution of security towards wireless ATM. *Operating Systems Review*, 36 (1):23–30, January 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Patiyoot:2002:SIW

[Pat02b] Danai Patiyoot. Security issues for wireless ATM networks. *Operating Systems Review*, 36(1):31–57, January 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Patarin:2003:LRR

[Pat03a] Jacques Patarin. Luby–Rackoff: 7 rounds are enough for security. In Boneh [Bon03], pages 513–529. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Paterson:2003:CCI

[Pat03b] Kenneth G. Paterson, editor. *Cryptography and Coding: 9th IMA International Conference, Cirencester, UK, December 16–18, 2003: Proceedings*, volume 2898 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-20663-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C76 2003. URL http:

//link.springer-ny.com/link/service/series/0558/tocs/t2898.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2898; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b93924.

Patarin:2004:SRF

[Pat04] Jacques Patarin. Security of random Feistel schemes with 5 or more rounds. In Franklin [Fra04], pages 106–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Paulson:2001:RBS

[Pau01] Lawrence C. Paulson. Relations between secrets: two formal analyses of the Yahalom protocol. *Journal of Computer Security*, 9 (3):197–216, ???? 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Paulson:2002:NBPb

[Pau02a] Linda Dailey Paulson. News briefs: Project promises accessible technology for the disabled; two efforts aim to upgrade mobile memory; new haptics approach lets parents-to-be “touch” their unborn children; prime breakthrough may improve encryption. *Computer*, 35 (10):26, October 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/dl/mags/co/2002/10/rx026.htm; http://csdl.computer.org/dl/mags/co/2002/10/rx026.pdf; http://www.cse.iitk.ac.in/news/primality.html.

Paulson:2002:NBR

[Pau02b] Linda Dailey Paulson. News briefs: Researchers upgrade Smart Card technology; new optical clock could synchronize chips; blind, deaf engineer develops computerized Braille machine. *Computer*, 35(12):25–27, December 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/dl/mags/co/2002/12/rz025.htm; http://csdl.computer.org/dl/mags/co/2002/12/rz025.pdf.

Paulson:2003:NBV

[Pau03] Linda Dailey Paulson. News briefs: Vendors push wireless LAN security; picturing a new encryption technique; think tank targets better software. *Computer*, 36(1): 28–30, January 2003. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://csdl.computer.org/dl/mags/co/2003/01/r1028.htm; http://csdl.computer.org/dl/mags/co/2003/01/r1028.pdf`.

Paulson:2009:NBT

[Pau09] Linda Dailey Paulson. News briefs: Technique makes strong encryption easier to use. *Computer*, 42(4):24–27, April 2009. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Praca:2001:SCS

[PB01] Denis Praca and Claude Barral. From smart cards to smart objects: the road to new smart technologies. *Computer Networks (Amsterdam, Netherlands: 1999)*, 36(4):381–389, July 16, 2001. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.elsevier.nl/gej-ng/10/15/22/61/28/26/abstract.html; http://www.elsevier.nl/gej-ng/10/15/22/61/28/26/article.pdf`.

Piva:2002:MCW

[PBB02] Alessandro Piva, Franco Bartolini, and Mauro Barni. Managing copyright: Watermark and cryptography algorithms. *IEEE Distributed Systems Online*, 3 (5):??, 2002. CODEN ???? ISSN 1541-4922 (print), 1558-1683 (electronic). URL `http://dsonline.computer.org/0205/features/w3piva.htm`.

Piva:2005:SRA

[PBC05] Alessandro Piva, Franco Bartolini, and Roberto Caldelli. Self recovery authentication of images in the DWT domain. *International Journal of Image and Graphics (IJIG)*, 5(1):149–??, January 2005. CODEN ???? ISSN 0219-4678.

Park:2000:CAP

[PBD00] DongGook Park, Colin Boyd, and Ed Dawson. Classification of authentication protocols: a practical approach. *Lecture Notes in Computer Science*, 1975:194–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750194.htm; http://link.springer-ny.com/link/service/series/0558/papers/1975/19750194.pdf`.

Peng:2005:SES

[PBD05] Kun Peng, Colin Boyd, and Ed Dawson. Simple and efficient shuffling with provable correctness and ZK privacy. In Shoup [Sho05a], pages 188–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Peng:2007:BZK

[PBD07] Kun Peng, Colin Boyd, and Ed Dawson. Batch zero-knowledge proof and verification and its applications. *ACM Transactions on Information and System Security*, 10(2):6:1–6:??, May 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Prattichizzo:2007:PIH

[PBM+07] Domenico Prattichizzo, Mauro Barni, Gloria Menegaz, Alessandro Formaglio, Hong Z. Tan, and Seungmoon Choi. Perceptual issues in haptic digital watermarking. *IEEE MultiMedia*, 14(3):84–91, July/September 2007. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Papadimitriou:2001:PSE

[PBMB01] S. Papadimitriou, T. Bountis, S. Mavroudi, and A. Bezerianos. A probabilistic symmetric encryption scheme for very fast secure communication based on chaotic systems of difference equations. *International journal of bifurcation and chaos in applied sciences and engineering*, 11 (12):3107–3115, 2001. CODEN IJBEE4. ISSN 0218-1274.

Perez:2007:URR

[PBTW07] O. Pérez, Y. Berviller, C. Tanougast, and S. Weber. The use of runtime reconfiguration on FPGA circuits to increase the performance of the AES algorithm implementation. *J.UCS: Journal of Universal Computer Science*, 13(3):349–362, ???? 2007. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_13_3/the_use_of_runtime.

Poulos:2008:TSE

[PBV08] Marios Poulos, George Bokos, and Fotios Vaioulis. Towards the semantic extraction of digital signatures for librarian image-identification purposes. *Journal of the American Society for Information Science and Technology: JASIST*, 59(5):708–718, March 2008. CODEN JASIEF. ISSN 1532-2882 (print), 1532-2890 (electronic).

Pucheral:2001:PSD

[PBVB01] Philippe Pucheral, Luc Bouganim, Patrick Valduriez, and Christophe Bobineau. PicoDBMS: Scaling down database techniques for the smartcard. *VLDB Journal: Very Large Data Bases*, 10(2–3):120–132, September 2001. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic). URL `http://link.springer.de/link/service/journals/00778/bibs/1010002/10100120.htm`; `http://link.springer.de/link/service/journals/00778/papers/1010002/10100120.pdf`.

Petrie:2000:NBI

[PC00] C. Petrie and J. Connelly. A noise-based IC random number generator for applications in cryptography. *IEEE Journal of Solid-State Circuits*, 47(5):615–621, ???? 2000. CODEN IJSCBC. ISSN 0018-9200 (print), 1558-173X (electronic).

Peikari:2004:SW

[PC04] Cyrus Peikari and Anton Chuvakin. *Security warrior*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, 2004. ISBN 0-596-00545-8. xvii + 531 pp. LCCN TK5105.59 .P44985 2004.

Park:2005:ISC

[PC05a] Choonsik Park and Seongtaek Chee, editors. *Information security and cryptology: ICISC 2004: 7th international conference, Seoul, Korea, December 2–3, 2004. Revised selected papers*, volume 3506 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-26226-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3506`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b137120`.

Park:2005:NDS

[PC05b] Je Hong Park and Seongtaek Chee. A note on digital signature scheme using a self-pairing map. *Applied Mathematics and Computation*, 169(1):472–475, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Perlner:2009:QRP

[PC09] Ray A. Perlner and David A. Cooper. Quantum resistant public key cryptography: a survey. In Seamons et al. [SMP+09], pages 85–93. ISBN 1-60558-474-6. LCCN QA76.9.A25 S954 2009. URL `http://portal.acm.org/toc.cfm?id=1527017&coll=portal&dl=ACM`.

Park:2003:ESA

[PCC03] Yongsu Park, Tae-Sun Chung, and Yookun Cho. An efficient stream authentication scheme using tree chaining. *Information Processing Letters*, 86(1):1–8, April 15, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Patarin:2001:QBL

[PCG01] Jacques Patarin, Nicolas Courtois, and Louis Goubin. QUARTZ, 128-bit long digital signatures. *Lecture Notes in Computer Science*, 2020:282–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200282.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200282.pdf`.

Park:2002:XQP

[PCK02] Sangwon Park, Yoonra Choi, and Hyoung-Joo Kim. XML query processing using signature and DTD. *Lecture Notes in Computer Science*, 2455:162–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2455/24550162.htm; http://link.springer-ny.com/link/service/series/0558/papers/2455/24550162.pdf`.

Park:2003:EMS

[PCS03] Jung Min Park, Edwin K. P. Chong, and Howard Jay Siegel. Efficient multicast stream authentication using erasure codes. *ACM Transactions on Information and System Security*, 6(2):258–285, May 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Pan:2007:IBS

[PCSM07] Jianping Pan, Lin Cai, Xuemin (Sherman) Shen, and Jon W. Mark. Identity-based secure collaboration in wireless ad hoc networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(3):853–865, February 21, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Peeters:2007:CES

[PD07] Johan Peeters and Paul Dyson. Cost-effective security. *IEEE Security & Privacy*, 5(3):85–87, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Petrakos:2009:CTA

[PDMS09] Nikolaos Petrakos, George W. Dinolt, James Bret Michael, and Pantelimon Stanica. Cube-type algebraic attacks on Wireless Encryption Protocols. *Computer*, 42(10):103–105, October 2009. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Peinado:2004:CLK

[Pei04] A. Peinado. Cryptanalysis of LHL-key authentication scheme. *Applied Mathematics and Computation*, 152 (3):721–724, May 13, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Peikert:2009:PKC

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In ACM [ACM09], pages 333–342. ISBN 1-60558-613-7. LCCN QA75.5 .A22 2009.

Pelzl:2006:PAC

[Pel06] Jan Pelzl. *Practical Aspects of Curve-based Cryptography and Cryptanalysis*. Europäischer Universitätsverlag, Bochum, Germany, 2006. ISBN 3-89966-189-3. 208 pp. LCCN ???? EUR 24.90. URL `http://verlag.rub.de/g9783899661897.html`.

Pemble:2001:CEW

[Pem01a] Matthew Pemble. Confidentiality: From encryption, to where? *Network Security*, 2001(4):10–11, April 1, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485801004172`.

Pemble:2001:SPA

[Pem01b] Matthew Pemble. A sceptical pigeon amongst the crypto cats: Report on the Edinburgh Financial Cryptographic Engineering Conference, 2001. *Network Security*, 2001(7):7–9, July 1, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485801007152`.

Perrine:2003:ECP

[Per03] Tom Perrine. The end of `crypt()` passwords ...

please? *;login: the USENIX Association newsletter*, 28 (6):??, December 2003. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/2003-12/pdfs/perrine.pdf.

Perlman:2005:EMD

[Per05a] Radia Perlman. The ephemerizer: Making data disappear. Technical report, Sun Labs, 16 Network Circle, Menlo Park, CA 94025, USA, 2005. 20 pp. URL http://www.research.sun.com/techrep/2005/smll-tr02005-140.pdf.

Perry:2005:DCP

[Per05b] Tekla S. Perry. DVD copy protection: take 2. *IEEE Spectrum*, 42(1):38–39, January 2005. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Petullo:2003:IEH

[Pet03] Mike Petullo. Implementing encrypted home directories. *Linux Journal*, 2003(112): 1, August 2003. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Petullo:2005:EYR

[Pet05] Mike Petullo. Encrypt your root filesystem. *Linux Journal*, 2005(129):4, January 2005. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Petzold:2008:ATG

[Pet08] Charles Petzold. *The annotated Turing: a guided tour through Alan Turing's historic paper on computability and the Turing Machine*. John Wiley and Sons, Inc., New York, NY, USA, 2008. ISBN 0-470-22905-5 (paperback). xii + 372 pp. LCCN QA267 .P48 2008.

Potter:2003:S

[PF03] Bruce Potter and Bob Fleck. *802.11 Security*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, 2003. ISBN 0-596-00290-4. xiii + 176 pp. LCCN TK5105.78 .P68 2003. US$34.95, CDN$54.95, UK£24.95. URL http://www.oreilly.com/catalog/80211security/.

Pfitzmann:2001:ACE

[Pfi01] Birgit Pfitzmann, editor. *Advances in cryptology: EUROCRYPT 2001: International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6–10, 2001: proceed-*

ings, volume 2045 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., April 25, 2001. ISBN 3-540-42070-3. LCCN QA76.9.A25 E964 2001; QA76.9.A25 E96 2001. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2045.htm; http://link.springer.de/link/service/series/0558/tocs/t2045.htm.

Phatak:2005:FMR

[PG05] Dhananjay Phatak and Tom Goff. Fast modular reduction for large wordlengths via one linear and one cyclic convolution. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL http://arith17.polito.it/final/paper-156.pdf.

Power:2007:SBB

[PGT07] E. Michael Power, Jonathan Gilhen, and Roland L. Trope. Setting boundaries at borders: Reconciling laptop searches and privacy. *IEEE Security & Privacy*, 5(2):72–75, March/April 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Provos:2003:HSI

[PH03] Niels Provos and Peter Honeyman. Hide and seek: An introduction to steganography. *IEEE Security & Privacy*, 1(3):32–44, May/June 2003. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://dlib.computer.org/sp/books/sp2003/pdf/j3032.pdf; http://www.computer.org/security/j3032abs.htm.

Phan:2004:IDC

[Pha04] Raphael C.-W. Phan. Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES). *Information Processing Letters*, 91(1):33–38, July 16, 2004. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Phan:2006:CTP

[Pha06] Raphael C.-W. Phan. Cryptanalysis of two password-based authentication schemes using smart cards. *Computers & Security*, 25(1):52–54, February 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404805001938.

Philpott:2006:ITD

[Phi06] Andrew Philpott. Identity theft — dodging the own-goals. *Network Security*, 2006(1):11–13, January 2006. CODEN

NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485806703233.

Paeng:2001:NPK

[PHK+01] Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik Park. New public key cryptosystem using finite non Abelian groups. In Kilian [Kil01a], pages 470–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390470.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390470.pdf.

Polk:2003:IIC

[PHM03] William T. Polk, Nelson E. Hastings, and Ambarish Malpani. IEEE Internet computing: Security track: Public key infrastructures that satisfy security goals. *IEEE Distributed Systems Online*, 4(7), 2003. CODEN ???? ISSN 1541-4922 (print), 1558-1683 (electronic). URL http://dsonline.computer.org/0307/f/wp4sec.htm.

Phoha:2001:SDI

[Pho01] Vir V. Phoha, editor. *The Springer Dictionary of Internet Security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 0-387-95261-6. 288 (est.) pp. LCCN TK5105.59 .P56 2002. US$39.95.

Pieprzyk:2003:FCS

[PHS03] Josef Pieprzyk, Thomas Hardjono, and Jennifer Seberry. *Fundamentals of computer security*. Monographs in theoretical computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 3-540-43101-2. xx + 677 pp. LCCN QA76.9.A25 P536 2003. US$69.95.

Pathak:2006:BFT

[PI06] Vivek Pathak and Liviu Iftode. Byzantine fault tolerant public key authentication in peer-to-peer systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 50(4):579–596, March 15, 2006. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Pietrzak:2005:CDI

[Pie05] Krzysztof Pietrzak. Composition does not imply adaptive security. In Shoup [Sho05a], pages

55–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Pinkas:2002:CTP

[Pin02] Benny Pinkas. Cryptographic techniques for privacy-preserving data mining. *ACM SIGKDD Explorations Newsletter*, 4(2):12–19, December 2002. CODEN ???? ISSN 1931-0145 (print), 1931-0153 (electronic).

Pinkas:2003:CTP

[Pin03] Benny Pinkas. Cryptographic techniques for privacy-preserving data mining. Report HPL-2003-22, Trusted Systems Laboratory, HP Laboratories Palo Alto, Palo Alto, CA, USA, January 29, 2003. URL http://www.hpl.hp.com/techreports/2003/HPL-2003-22.html. To be published in SIGKDD Explorations, Volume 4, Issue 2.

Pincock:2006:CHC

[Pin06] Stephen Pincock. *Codebreaker: the history of codes and ciphers, from the ancient pharaohs to quantum cryptography*. Walker, New York, NY, USA, 2006. ISBN 0-8027-1547-8. 176 pp. LCCN Z104 .P56 2006. URL http://www.loc.gov/catdir/enhancements/fy0730/2007310362-b.html; http://www.loc.gov/catdir/enhancements/fy0730/2007310362-d.html.

Piper:2003:RCS

[Pip03] Fred Piper. Reseacrh in cryptography and security mechanisms. *Computers & Security*, 22(1):22–25, January 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803001044.

Park:2001:NDW

[PJH01] Ji Hwan Park, Sook Ee Jeong, and Young Huh. A new digital watermarking for text document images using diagonal profile. *Lecture Notes in Computer Science*, 2195: 748–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950748.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950748.pdf.

Park:2001:RFW

[PJK01] Ji Hwan Park, Sook Ee Jeong, and Chang Soo Kim. Robust and fragile watermarking techniques for documents using bi-directional diagonal profiles. *Lecture Notes in Computer Science*, 2229:483–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290483.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290483.pdf.

Poh:2001:HBP

[PK01] Norman Poh and Jerzy Korczak. Hybrid biometric person authentication using face and voice features. *Lecture Notes in Computer Science*, 2091:348–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2091/20910348.htm; http://link.springer-ny.com/link/service/series/0558/papers/2091/20910348.pdf.

Petitcolas:2003:DWF

[PK03] Fabien A. P. Petitcolas and Hyoung Joong Kim, editors. *Digital watermarking: First International Workshop, IWDW 2002, Seoul, Korea, November 21–22, 2002: Revised Papers*, volume 2613. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-01217-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I939 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2613.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2613. Also available via the World Wide Web.

Park:2001:CSC

[PKBD01] DongGook Park, JungJoon Kim, Colin Boyd, and Ed Dawson. Cryptographic salt: a countermeasure against denial-of-service attacks. *Lecture Notes in Computer Science*, 2119:334–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190334.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190334.pdf.

Park:2005:CZA

[PKH05] Je Hong Park, Bo Gyeong Kang, and Jae Woo Han. Cryptanalysis of Zhou et al.'s proxy-protected signature schemes. *Applied Mathematics and Computation*, 169(1):192–197, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Park:2001:DNP

[PL01] Hee-Un Park and Im-Yeong Lee. A digital nominative proxy signature scheme for mobile communication. *Lecture Notes in Computer Science*, 2229: 451–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290451.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290451.pdf.

Pliam:2001:PTU

[Pli01] John O. Pliam. A polynomial-time universal security amplifier in the class of block ciphers. *Lecture Notes in Computer Science*, 2012: 169–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120169.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120169.pdf.

Pon:2005:MDS

[PLJ05a] Shun-Fu Pon, Erl-Huei Lu, and Albert B. Jeng. Meta-He digital signatures based on factoring and discrete logarithms. *Applied Mathematics and Computation*, 165(1):171–176, June 6, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Pon:2005:OPK

[PLJ05b] Shun-Fu Pon, Erl-Huei Lu, and Albert B. Jeng. One private-key for all DL-based cryptosystems. *Applied Mathematics and Computation*, 170(1):666–672, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Peris-Lopez:2010:CSP

[PLSvdLE10] Pedro Peris-Lopez, Enrique San Millán, Jan C. A. van der Lubbe, and Luis A. Entrena. Cryptographically secure pseudo-random bit generator for RFID tags. In *2010 International Conference for Internet Technology and Secured Transac-*

tions (ICITST), pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5678035`.

Pfleeger:2007:IBC

[PLW07] Shari Lawrence Pfleeger, Martin Libicki, and Michael Webber. I'll buy that! cybersecurity in the Internet marketplace. *IEEE Security & Privacy*, 5(3):25–31, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Paulson:2000:NBU

[PM00] Linda Dailey Paulson and Orren Merton. News briefs: U.S. picks new encryption standard; better software with open source; taking a SIP of Internet telephony; schools may hold valuable spectrum; getting a feel for the Web. *Computer*, 33(12): 20–23, December 2000. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co2000/pdf/rz020.pdf`.

Piper:2002:CVS

[PM02] Fred Piper and Sean Murphy. *Cryptography: a Very Short Introduction*, volume 68 of *Very short introductions*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2002. ISBN 0-19-280315-8. 142 pp. LCCN Z103 .P56 2002. UK£6.99.

Pang:2008:AQR

[PM08] HweeHwa Pang and Kyriakos Mouratidis. Authenticating the query results of text search engines. *Proceedings of the VLDB Endowment*, 1(1):126–137, August 2008. CODEN ???? ISSN 2150-8097.

Peyravian:2000:MBB

[PMRZ00] Mohammad Peyravian, Stephen M. Matyas, Allen Roginsky, and Nevenko Zunic. Multiparty biometric-based authentication. *Computers & Security*, 19(4):369–374, April 1, 2000. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404800040256`.

Pohlmann:2001:SCA

[Poh01] Norbert Pohlmann. Smart cards: The authenticated solution for e-business user. *Network Security*, 2001(4): 12–15, April 1, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485801004184`.

Pointcheval:2000:CCS

[Poi00] David Pointcheval. Chosen-ciphertext security for any one-way cryptosystem. *Lecture Notes in Computer Science*, 1751:129–146, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pointcheval:2002:PSP

[Poi02] David Pointcheval. Practical security in public-key cryptography. *Lecture Notes in Computer Science*, 2288:1–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880001.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2288/22880001.pdf`.

Pointcheval:2006:TCC

[Poi06] David Pointcheval, editor. *Topics in Cryptology — CT-RSA 2006: The Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 13–17, 2006, proceedings*, volume 3860 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-31033-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3860`.

Poole:2003:NSP

[Poo03] Owen Poole. *Network Security: a Practical Guide*. Butterworth-Heinemann, Boston, MA, USA, 2003. ISBN 0-7506-5033-8. xi + 212 pp. LCCN TK5105.59 .P66 2003. US$47.95. URL `http://www.loc.gov/catdir/description/els051/2004315747.html`; `http://www.loc.gov/catdir/toc/els051/2004315747.html`.

Pornin:2001:THE

[Por01] T. Pornin. Transparent harddisk encryption. *Lecture Notes in Computer Science*, 2162:273–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620273.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2162/21620273.pdf`.

Porras:2006:PEG

[Por06] Phillip A. Porras. Privacy-enabled global threat monitoring. *IEEE Security & Privacy*, 4(6):60–63, November/December 2006.

CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Potter:2003:WAO

[Pot03] Bruce Potter. Wireless authentication options for up and down the Stack. *Network Security*, 2003(6):4–5, June 2003. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S135348580300607X`.

Potter:2005:QCS

[Pot05] Bruce Potter. Quantum crypto: Star trek or real science? *Network Security*, 2005(7):4–5, July 2005. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485805702579`.

Potter:2006:CKM

[Pot06] Bruce Potter. Cryptographic key management for the masses. *Network Security*, 2006(12):13–14, December 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485806704639`.

Potter:2007:CWW

[Pot07] Bruce Potter. Converging wired and wireless authentication. *Network Security*, 2007(10):18–20, October 2007. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S135348580770096X`.

Pfleeger:2003:SC

[PP03] Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in computing*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, third edition, 2003. ISBN 0-13-035548-8. xxix + 746 pp. LCCN QA76.9.A25 P45 2003.

Paul:2006:SSC

[PP06a] Souradyuti Paul and Bart Preneel. On the (in)security of stream ciphers based on arrays and modular addition. *Lecture Notes in Computer Science*, 4284: 69–83, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11935230_5.pdf`.

Popp:2006:CTT

[PP06b] Robert Popp and John Poindexter. Countering terrorism through information and privacy protection technologies. *IEEE Security & Privacy*, 4(6): 18–27, November/December 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Pfleeger:2007:SC

[PP07] Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in computing*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, fourth edition, 2007. ISBN 0-13-239077-9 (hardcover). xxiii + 845 pp. LCCN QA76.9.A25 P45 2006. URL http://www.loc.gov/catdir/toc/ecip0619/2006026798.html.

Paar:2009:UCT

[PP09] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 3-642-04100-0 (hardcover), 3-642-04101-9 (paperback). xviii + 372 pp. LCCN A76.9.A25 P437 2009.

Pellikaan:1996:AGC

[PPV96] R. Pellikaan, M. Perret, and S. G. Vladut, editors. *Arithmetic, geometry, and coding theory: proceedings of the international conference held at Centre international de rencontres mathématiques (CIRM), Luminy, France, June 28–July 2, 1993*. Walter de Gruyter, New York, NY, USA, 1996. ISBN 3-11-014616-9. LCCN QA268 .A75 1996. UK£102.45.

Pereira:2003:SAU

[PQ03a] Olivier Pereira and Jean-Jacques Quisquater. Some attacks upon authenticated group key agreement protocols. *Journal of Computer Security*, 11(4):555–580, ???? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Piret:2003:DFA

[PQ03b] Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In Walter et al. [WKP03], pages 77–88. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Pereira:2006:IBS

[PQ06] Olivier Pereira and Jean-Jacques Quisquater. On the impossibility of building secure Cliques-type authenticated group key agreement protocols. *Journal of Computer Security*, 14 (2):197–246, ???? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Picard:2001:NNF

[PR01] Justin Picard and Arnaud Robert. Neural networks functions for public key watermarking. *Lecture Notes in Computer Science*, 2137: 142–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370142.htm; http://link.springer-ny.com/link/service/series/0558/papers/2137/21370142.pdf.

Pass:2005:NIC

[PR05] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. In ACM [ACM05c], pages 533–542. ISBN 1-58113-960-8. LCCN QA75.5 A22 2005.

Pass:2008:NIC

[PR08] Rafael Pass and Alon Rosen. New and improved constructions of nonmalleable cryptographic protocols. *SIAM Journal on Computing*, 38 (2):702–752, ???? 2008. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Preneel:2000:ACE

[Pre00] Bart Preneel, editor. *Advances in cryptology: EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14–18, 2000: proceedings*, volume 1807 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-67517-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1807.

Preneel:2001:NES

[Pre01] Bart Preneel. New European Schemes for Signature, Integrity and Encryption (NESSIE): a status report. *Lecture Notes in Computer Science*, 2274: 297–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740297.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740297.pdf.

Preneel:2002:NEA

[Pre02a] Bart Preneel. NESSIE: a European approach to evaluate cryptographic algorithms. *Lecture Notes in Computer Science*, 2355: 267–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550267.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550267.pdf; https://www.cosic.esat.kuleuven.be/publications/article-82.ps.

Preneel:2002:NPT

[Pre02b] Bart Preneel. The NESSIE Project: Towards new cryptographic algorithms. Report ??, Katholieke Univ. Leuven, Dept. Electrical Engineering-ESAT, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium, November 25, 2002. URL http://www.stork.eu.org/papers/03_nessiev2.pdf.

Preneel:2002:TCC

[Pre02c] Bart Preneel, editor. *Topics in cryptology, CT-RSA 2002: the Cryptographers' Track at RSA Conference 2002, San Jose, CA, USA, February 18–22, 2002: Proceedings*, volume 2271 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-43224-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 R753 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2271.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2271.

Preneel:2007:SRD

[Pre07] Bart Preneel. A survey of recent developments in cryptographic algorithms for smart cards. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(9):2223–2233, June 20, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Price:2000:NCH

[Pri00] Dick Price. News: CAIDA helps train network engineers, 109-bit cryptographic key cracked, LosLobos–Linux supercluster. *IEEE Concurrency*, 8(2):4–7, April/June 2000. CODEN IECMFX. ISSN 1092-3063 (print), 1558-0849 (electronic). URL http://dlib.computer.org/pd/books/pd2000/pdf/p2004.pdf.

Provos:2000:EVM

[Pro00] Niels Provos. Encrypting virtual machine. In USENIX [USE00d], page ?? ISBN 1-880446-18-9. LCCN ???? URL `http://www.usenix.org/publications/library/proceedings/sec2000/provos.html`.

Provos:2001:DAS

[Pro01] Niels Provos. Defending against statistical steganalysis. In USENIX [USE01c], page ?? ISBN 1-880446-18-9, 1-880446-07-3. LCCN QA76.9.A25 U565 2001. URL `http://www.usenix.org/publications/library/proceedings/sec01/provos.html`.

Paun:2004:CTT

[PRS04] Gheorghe Păun, Grzegorz Rozenberg, and Arto Salomaa, editors. *Current trends in theoretical computer science: the challenge of the new century*. World Scientific Publishing Co., Singapore; Philadelphia, PA, USA; River Edge, NJ, USA, 2004. ISBN 981-238-783-8 (set), 981-238-966-0 (vol. 1), 981-238-965-2 (vol. 2). ???? pp. LCCN QA76 .C878 2004.

Poupard:2000:FER

[PS00] Guillaume Poupard and Jacques Stern. Fair encryption of RSA keys. *Lecture Notes in Computer Science*, 1807:172–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070172.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070172.pdf`.

Parker:2001:RKC

[PS01a] Andrew T. Parker and Kevin M. Short. Reconstructing the keystream from a chaotic encryption scheme. *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, 48(5):624–635, 2001. CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic).

Pfitzmann:2001:SEC

[PS01b] Birgit Pfitzmann and Ahmad-Reza Sadeghi. Self-escrowed cash against user blackmailing. *Lecture Notes in Computer Science*, 1962:42–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620042.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620042.pdf`.

Pornin:2001:SHT

[PS01c] Thomas Pornin and Jacques Stern. Software-hardware trade-offs: Application to A5/1 cryptanalysis. *Lecture Notes in Computer Science*, 1965:318–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650318.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650318.pdf.

Padro:2002:LBI

[PS02a] Carles Padró and Germán Sáez. Lower bounds on the information rate of secret sharing schemes with homogeneous access structure. *Information Processing Letters*, 83(6):345–351, September 30, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Pomerance:2002:SOC

[PS02b] Carl Pomerance and Igor E. Shparlinski. Smooth orders and cryptographic applications. *Lecture Notes in Computer Science*, 2369: 338–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2369/23690338.htm; http://link.springer-ny.com/link/service/series/0558/papers/2369/23690338.pdf.

Page:2004:PCA

[PS04a] D. Page and N. P. Smart. Parallel cryptographic arithmetic using a redundant Montgomery representation. *IEEE Transactions on Computers*, 53(11):1474–1482, November 2004. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1336767.

Park:2004:UUC

[PS04b] Jaehong Park and Ravi Sandhu. The UCON$_{ABC}$ usage control model. *ACM Transactions on Information and System Security*, 7 (1):128–174, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Prabhakaran:2004:NNS

[PS04c] Manoj Prabhakaran and Amit Sahai. New notions of security: achieving universal composability without trusted setup. In ACM [ACM04b], pages 242–251. ISBN 1-58113-852-0. LCCN QA75.5 .A22 2004.

Prabhakaran:2005:RES

[PS05] Manoj Prabhakaran and Amit Sahai. Relaxing environmental security: Monitored functionalities and client-server computation. In Kilian [Kil05], pages 104–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Phan:2006:FDB

[PS06] R. C.-W. Phan and M. U. Siddiqi. A framework for describing block cipher cryptanalysis. *IEEE Transactions on Computers*, 55(11): 1402–1409, November 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1705449.

Park:2008:SRB

[PS08a] Taejoon Park and Kang G. Shin. Secure routing based on distributed key sharing in large-scale sensor networks. *ACM Transactions on Embedded Computing Systems*, 7(2):20:1–20:??, February 2008. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Pavlou:2008:FAD

[PS08b] Kyriacos E. Pavlou and Richard T. Snodgrass. Forensic analysis of database tampering. *ACM Transactions on Database Systems*, 33(4): 30:1–30:??, November 2008. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Park:2002:SRL

[PSC+02] Sangwoo Park, Soo Hak Sung, Seongtaek Chee, E-Joong Yoon, and Jongin Lim. On the security of Rijndael-like structures against differential and linear cryptanalysis. *Lecture Notes in Computer Science*, 2501:176–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010176.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010176.pdf.

Pareschi:2009:PAC

[PSG+09] F. Pareschi, G. Scotti, L. Giancane, R. Rovatti, G. Setti, and A. Trifiletti. Power analysis of a chaos-based random number generator for cryptographic security. In *2009. ISCAS*

2009. IEEE International Symposium on Circuits and Systems, pages 2858–2861. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5118398.

Petit:2008:BCB

[PSP+08] C. Petit, F. Standaert, O. Pereira, T. Malkin, and M. Yung. A block cipher based pseudo random number generator secure against side-channel key recovery. In ????, editor, *ASIAN ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, pages 56–65. ACM Press, New York, NY 10036, USA, 2008. ISBN ???? LCCN ????

Preneel:2006:SAC

[PT06] Bart Preneel and Stafford Tavares, editors. *Selected Areas in Cryptography: 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11–12, 2005, Revised Selected Papers*, volume 3897 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-33108-5 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3897.

Pang:2008:VCR

[PT08] Hweehwa Pang and Kian-Lee Tan. Verifying Completeness of Relational Query Answers from Online Servers. *ACM Transactions on Information and System Security*, 11(2):5:1–5:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Pfleeger:2007:GEI

[PTP07] Shari Lawrence Pfleeger, Roland L. Trope, and Charles C. Palmer. Guest Editors' introduction: Managing organizational security. *IEEE Security & Privacy*, 5(3):13–15, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Pucella:2003:JRB

[Puc03] Riccardo Pucella. Joint review of *Foundations of Cryptography: Basic Tools*, by O. Goldreich. Cambridge University Press, and *Modelling and Analysis of Security Protocols*, by P. Ryan and S. Schneider. Addison Wesley. *ACM SIGACT News*, 34(4):26–31, December 2003. CODEN

SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Gol01b].

Pucella:2006:SCC

[Puc06] Riccardo Pucella. Security and composition of cryptographic protocols: a tutorial (Part I). *ACM SIGACT News*, 37(3):67–92, September 2006. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Pucella:2007:Ib

[Puc07] Riccardo Pucella. Introduction. *ACM SIGACT News*, 38(4):64, December 2007. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL `http://doi.acm.org/10.1145/1345189.1345204`.

Puzmanova:2004:RWF

[Puz04] Rita Puzmanova. Review of *Wi-Foo: The Secrets of Wireless Hacking* by Andrew Vladimirov, Konstantin V. Gravrilenko, and Andrei A. Mikhailovsky. Pearson Education, 2004, ISBN 0-321-20217-1. *ACM Queue: Tomorrow's Computing Today*, 2(8):70, November 2004. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Page:2006:FAP

[PV06a] D. Page and F. Vercauteren. A fault attack on pairing-based cryptography. *IEEE Transactions on Computers*, 55(9):1075–1080, September 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1668035`.

Paillier:2006:TOW

[PV06b] Pascal Paillier and Jorge L. Villar. Trading one-wayness against chosen-ciphertext security in factoring-based encryption. *Lecture Notes in Computer Science*, 4284: 252–266, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11935230_17.pdf`.

Phillips:2001:GRI

[PvS01] Deborah M. Phillips and Hans A. von Spakovsky. Gauging the risks of Internet elections. *Communications of the Association for Computing Machinery*, 44(1):73, January 2001. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/citations/journals/cacm/2001-44-1/p73-phillips/`. See correction [CTBA+01].

Pang:2005:NMS

[PW05] Liao-Jun Pang and Yu-Min Wang. A new

(tn) multi-secret sharing scheme based on Shamir's secret sharing. *Applied Mathematics and Computation*, 167(2):840–848, August 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300304005338.

Peikert:2008:LTF

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In ACM [ACM08], pages 187–196. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Pelzl:2003:HCC

[PWGP03] Jan Pelzl, Thomas Wollinger, Jorge Guajardo, and Christof Paar. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. In Walter et al. [WKP03], pages 351–365. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Patrick:2005:FCD

[PY05] Andrew S. Patrick and Moti Yung, editors. *Financial cryptography and data security: 9th international conference, FC 2005, Roseau, The Commonwealth of Dominica, February 28–March 3, 2005: revised papers*, volume 3570 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-26656-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 2005; HG1710 .F35 2005eb; HG1710; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3570.

Paterson:2006:LTT

[PY06] Kenneth G. Paterson and Arnold K. L. Yau. Lost in translation: Theory and practice in cryptography. *IEEE Security & Privacy*, 4 (3):69–72, May/June 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Palanivel:2008:MPA

[PY08] S. Palanivel and B. Yegnanarayana. Multimodal person authentication using speech, face and visual speech. *Computer Vi-*

sion and Image Understanding: CVIU, 109(1):44–55, January 2008. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic).

Pieprzyk:2001:CPS

[PZ01] J. Pieprzyk and X.-M. Zhang. Cheating prevention in secret sharing over GF(pt). *Lecture Notes in Computer Science*, 2247: 79–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470079.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470079.pdf`.

Pieprzyk:2002:CPL

[PZ02a] Josef Pieprzyk and Xian-Mo Zhang. Cheating prevention in linear secret sharing. *Lecture Notes in Computer Science*, 2384: 121–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840121.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840121.pdf`.

Pieprzyk:2002:CCI

[PZ02b] Josef Pieprzyk and Xian-Mo Zhang. Constructions of cheating immune secret sharing. *Lecture Notes in Computer Science*, 2288: 226–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880226.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880226.pdf`.

Pecho:2009:APW

[PZDH09] P. Pecho, F. Zboril, Jr., M. Drahansky, and P. Hanacek. Agent platform for wireless sensor network with support for cryptographic protocols. *J.UCS: Journal of Universal Computer Science*, 15(5):992–??, ???? 2009. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_15_5/agent_platform_for_wireless`.

Peng:2009:DIE

[PZL09] Jun Peng, Du Zhang, and Xiaofeng Liao. A digital image encryption algorithm based on hyper-chaotic cellular neural network. *Fundamenta Informaticae*, 90 (3):269–282, March 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Qian:2005:CLT

[QCB05a] Haifeng Qian, ZhenFu Cao, and Haiyong Bao. Cryptanalysis of Li–Tzeng–Hwang's improved signature schemes based on factoring and discrete logarithms. *Applied Mathematics and Computation*, 166(3):501–505, July 26, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Qian:2005:SPL

[QCB05b] Haifeng Qian, Zhenfu Cao, and Haiyong Bao. Security of Pon–Lu–Jeng's Meta-He digital signature schemes. *Applied Mathematics and Computation*, 170(1):724–730, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Quisquater:2005:SCC

[QPV05] Michaël Quisquater, Bart Preneel, and Joos Vandewalle. Spectral characterization of cryptographic Boolean functions satisfying the (extended) propagation criterion of degree l and order k. *Information Processing Letters*, 93(1):25–28, January 16, 2005. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Quisquater:2000:SCR

[QS00] J.-J. Quisquater and Bruce Schneier, editors. *Smart card research and applications: third international conference, CARDIS'98, Louvain-la-Neuve, Belgium, September 1998: proceedings*, volume 1820 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-67923-5. LCCN TK7895.S62 C36 1998.

Quisquater:2001:EAE

[QS01] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic analysis (EMA): Measures and countermeasures for smart cards. *Lecture Notes in Computer Science*, 2140:200–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400200.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400200.pdf.

Quisquater:2002:CTM

[QSR+02] Jean-Jacques Quisquater, François-Xavier Standaert, Gael Rouvroy, Jean-Pierre David, and Jean-Didier Legat. A cryptanalytic time-memory tradeoff: First

FPGA implementation. *Lecture Notes in Computer Science*, 2438:780–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2438/24380780.htm; http://link.springer-ny.com/link/service/series/0558/papers/2438/24380780.pdf.

Qu:2001:KPW

[Qu01] Gang Qu. Keyless public watermarking for intellectual property authentication. *Lecture Notes in Computer Science*, 2137:96–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370096.htm; http://link.springer-ny.com/link/service/series/0558/papers/2137/21370096.pdf.

Raikhel:2000:DF

[Rai00] Eugene Raikhel. Decoding the forecast. *Scientific American*, 283(3s):20–??, March 2000. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Rajsbaum:2006:ASNb

[Raj06] Sergio Rajsbaum. ACM SIGACT news distributed computing column 24. *ACM SIGACT News*, 37(4):58–84, December 2006. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL http://doi.acm.org/10.1145/1189056.1189074.

Roman:2007:SCP

[RAL07] Rodrigo Roman, Cristina Alcaraz, and Javier Lopez. A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes. *Mobile Networks and Applications*, 12(4):231–244, August 2007. CODEN ???? ISSN 1383-469X.

Ramesh:2001:TAE

[Ram01] D. Ramesh. A twin algorithm for efficient generation of digital signatures. *Lecture Notes in Computer Science*, 2247:267–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470267.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470267.pdf.

Rand:1955:MRD

[Ran55] Rand Corporation. *A Million Random Digits With 100,000 Normal Deviates*. Free Press, Glencoe, IL, USA, 1955. ISBN 0-02-925790-5. xxv + 400 + 200 pp. LCCN QA276.5 .R3. Reprinted in 1966 and 2001 [Ran01]. See also [Tip27].

Rand:2001:MRD

[Ran01] Rand Corporation. *A Million Random Digits With 100,000 Normal Deviates*. Rand Corporation, Santa Monica, CA, USA, 2001. ISBN 0-8330-3047-7. xxv + 400 + 200 pp. LCCN QA276.25 .M55 2001. See also [Ran55].

Rijmen:2001:WHF

[RB01] Vincent Rijmen and Paulo S. L. M. Barreto. The WHIRLPOOL hash function. World-Wide Web document, 2001. URL `http://paginas.terra.com.br/informatica/paulobarreto/WhirlpoolPage.html`; `http://planeta.terra.com.br/informatica/paulobarreto/whirlpool.zip`.

Rogaway:2003:OBC

[RBB03] Phillip Rogaway, Mihir Bellare, and John Black. OCB: a block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security*, 6 (3):365–403, August 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Rijmen:2008:RSA

[RBF08] Vincent Rijmen, Paulo S. L. M. Barreto, and Décio L. Gazzoni Filho. Rotation symmetry in algebraically generated cryptographic substitution tables. *Information Processing Letters*, 106(6):246–250, June 15, 2008. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Roth:2001:EJA

[RC01] Volker Roth and Vania Conan. Encrypting Java archives and its application to mobile agent security. *Lecture Notes in Computer Science*, 1991: 229–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1991/19910229.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1991/19910229.pdf`.

Rogers:2005:NSE

[RC05] Russ Rogers and Bryan Cunningham, editors. *Network security evaluation using the NSA IEM*. Syngress Publishing, Inc., Rockland, MA, USA, 2005. ISBN 1-59749-035-0. xxvi + 437 pp. LCCN TK5105.59 .N33 2005.

Rubin:2006:CSE

[RC06] Bradley S. Rubin and Donald Cheung. Computer security education and research: Handle with care. *IEEE Security & Privacy*, 4(6): 56–59, November/December 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Reed:2000:ANA

[RCBL00] Benjamin C. Reed, Edward G. Chron, Randal C. Burns, and Darrell D. E. Long. Authenticating network-attached storage. *IEEE Micro*, 20(1):49–57, January/February 2000. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL `http://dlib.computer.org/mi/books/mi2000/pdf/m1049.pdf; http://www.computer.org/micro/mi2000/m1049abs.htm`.

Rubin:2005:ARS

[RCG+05] Shai Rubin, Mihai Christodorescu, Vinod Ganapathy, Jonathon T. Giffin, Louis Kruger, Hao Wang, and Nicholas Kidd. An auctioning reputation system based on anomaly. In Meadows and Syverson [MS05b], pages 270–279. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Rangan:2001:PCI

[RD01] C. Pandu Rangan and C. Ding, editors. *Progress in cryptology: INDOCRYPT 2001: Second International Conference on Cryptology in India, Chennai, India, December 16–20, 2001: proceedings*, volume 2247 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-43010-5. LCCN QA76.9.A25 I5535 2001. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2247.htm`.

Renaud:2009:VPC

[RD09] Karen Renaud and Antonella De Angeli. Visual passwords: cure-all or snake-oil? *Communications of the Association for Computing Machinery*, 52(12): 135–140, December 2009. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Rudra:2001:ERE

[RDJ+01] A. Rudra, P. K. Dubey, C. S. Jutla, V. Kumar, J. R. Rao, and P. Rohatgi. Efficient Rijndael encryption implementation with composite field arithmetic. *Lecture Notes in Computer Science*, 2162: 171–??, 2001. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620171.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620171.pdf.

Romao:2001:SMA

[RdS01] Artur Romão and Miguel Mira da Silva. Secure mobile agent digital signatures with proxy certificates. *Lecture Notes in Computer Science*, 2033:206–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2033/20330206.htm; http://link.springer-ny.com/link/service/series/0558/papers/2033/20330206.pdf.

Rankl:2000:SCH

[RE00] W. (Wolfgang) Rankl and W. Effing. *Smart card handbook*. John Wiley and Sons, Inc., New York, NY, USA, second edition, 2000. ISBN 0-471-98875-8. xxviii + 746 pp. LCCN TK7895.S62 R3613 2000.

Riley:2002:CBR

[RE02] K. Jonathan Riley and John P. Eakins. Content-based retrieval of historical watermark images: I-tracings. *Lecture Notes in Computer Science*, 2383: 253–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2383/23830253.htm; http://link.springer-ny.com/link/service/series/0558/papers/2383/23830253.pdf.

Rankl:2003:SCH

[RE03] W. (Wolfgang) Rankl and W. Effing. *Smart Card Handbook*. John Wiley and Sons, Inc., New York, NY, USA, third edition, 2003. 1120 pp.

Reeds:2001:BRB

[Ree01] Jim Reeds. Book review: *The Code Book: the Evolution of Secrecy from Mary Queen Of Scots to Quantum Cryptography*, by Simon Singh. Anchor Books. *ACM SIGACT News*, 32(2): 6–11, June 2001. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Sin99].

Reese:2003:ELD

[Ree03] R. A. Reese. Extreme lawsuits [digital copyright]. *IEEE Spectrum*, 40(5):23–25, May 2003. CODEN IEESAM. ISSN 0018-9235

(print), 1939-9340 (electronic).

Regev:2003:NLB

[Reg03] Oded Regev. New lattice based cryptographic constructions. In ACM [ACM03b], pages 407–416. ISBN ???? LCCN QA75.5 .A22 2003. ACM order number 508030.

Regev:2004:NLB

[Reg04] Oded Regev. New lattice-based cryptographic constructions. *Journal of the ACM*, 51(6):899–942, November 2004. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Regev:2005:LLE

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In ACM [ACM05c], pages 84–93. ISBN 1-58113-960-8. LCCN QA75.5 A22 2005.

Regev:2009:LLE

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34:1–34:40, September 2009. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Ren:2009:CWT

[Ren09] Jian Ren. A cryptographic watermarking technique for multimedia signals. *Advances in Computational Mathematics*, 31(1–3):267–281, October 2009. CODEN ACMHEX. ISSN 1019-7168 (print), 1572-9044 (electronic). URL `http://link.springer.com/article/10.1007/s10444-008-9096-1`.

Rescorla:2001:IOPa

[Res01a] Eric Rescorla. An introduction to OpenSSL programming, Part I of II. *Linux Journal*, 89:74, 76–78, 80, 82–83, September 2001. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Rescorla:2001:IOPb

[Res01b] Eric Rescorla. An introduction to OpenSSL programming, Part II of II. *Linux Journal*, 92:??, December 2001. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL `http://www.linuxjournal.com/article.php?sid=5487`. Web only.

Reynard:2001:SCB

[Rey01] Robert Reynard. Secret code breaker online. World-Wide Web document, September 2001. URL `http://codebreaker.dids.com/`.

Rodwell:2007:NIBa

[RFR07a] P. M. Rodwell, S. M. Furnell, and P. L. Reynolds. A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. *Computers & Security*, 26(7–8):468–478, December 2007. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404807001095.

Rodwell:2007:NIBb

[RFR07b] P. M. Rodwell, S. M. Furnell, and P. L. Reynolds. A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. *Computers & Security*, 26(7–8):468–478, December 2007. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404807001095.

Rodwell:2007:NIBc

[RFR07c] P. M. Rodwell, S. M. Furnell, and P. L. Reynolds. A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. *Computers & Security*, 26(7–8):468–478, December 2007. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404807001095.

Ringenburg:2005:PFS

[RG05] Michael F. Ringenburg and Dan Grossman. Preventing format-string attacks via automatic and efficient dynamic checking. In Meadows and Syverson [MS05b], pages 354–363. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Rotondi:2006:CHA

[RG06] Guido Rotondi and Gianpiero Guerrera. A consistent history authentication protocol. *ACM SIGSOFT Software Engineering Notes*, 31 (3):1–7, May 2006. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Ren:2009:FCS

[RG09] Yanli Ren and Dawu Gu. Fully CCA2 secure identity based broadcast encryption without random oracles. *Information Processing Letters*, 109(11):527–533, May 16, 2009. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Rose:2006:CSP

[RGX06] Gregory Gordon Rose, Alexander Gantman, and

Lu Xiao. Cryptographically secure pseudo-random number generator. United States Patent 8,019,802., August 23, 2006. URL http:www.google.com/patents/US8019802.

Rojas:2000:FCH

[RH00] Raúl Rojas and Ulf Hashagen, editors. *The first computers: history and architectures*. History of computing. MIT Press, Cambridge, MA, USA, 2000. ISBN 0-262-18197-5 (hardcover), 0-585-35535-5 (electronic). xii + 457 pp. LCCN QA76.17 .F57 2000.

Roscoe:2002:TBC

[RH02] Timothy Roscoe and Steven Hand. Transaction-based charging in mnemosyne: a peer-to-peer steganographic storage system. *Lecture Notes in Computer Science*, 2376:335–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2376/23760335.htm; http://link.springer.de/link/service/series/0558/papers/2376/23760335.pdf.

Rafaeli:2003:SKM

[RH03] Sandro Rafaeli and David Hutchison. A survey of key management for secure group communication. *ACM Computing Surveys*, 35(3):309–329, September 2003. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Rhinelander:2003:DIE

[Rhi03] Jason P. Rhinelander. Design and implementation of encryption algorithms in a coarse grain reconfigurable environment. Thesis (M. Eng.), Memorial University of Newfoundland, St. Johns, Newfoundland, Canada, 2003.

Rich:2007:ATS

[Ric07] Donald Rich. Authentication in transient storage device attachments. *Computer*, 40(4):102–104, April 2007. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Riezenman:2000:CSB

[Rie00] M. J. Riezenman. Cellular security: better, but foes still lurk. *IEEE Spectrum*, 37(6):39–42, June 2000. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Riebeck:2003:SCC

[Rie03] H. Riebeck. A second coffin for chernobyl. *IEEE Spectrum*, 40(3):30–31, March 2003. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Rila:2002:DAB

[Ril02] Luciano Rila. Denial of access in biometrics-based authentication systems. *Lecture Notes in Computer Science*, 2437:19–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2437/24370019.htm; http://link.springer.de/link/service/series/0558/papers/2437/24370019.pdf.

Risen:2006:SWS

[Ris06] James Risen. *State of war: the secret history of the CIA and the Bush administration*. Free Press, New York, NY, USA, 2006. ISBN 0-7432-7066-5. 240 pp. LCCN ????

Rivest:2003:TLE

[Riv03] Ronald L. Rivest. Turing Lecture on early RSA days. World-Wide Web slide presentation, video, and audio., 2003. URL http://www.acm.org/turingawardlecture/RSA/.

Renner:2005:UCP

[RK05] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In Kilian [Kil05], pages 407–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171.

Ruan:2006:NSC

[RK06] X. Ruan and R. S. Katti. A new source coding scheme with small expected length and its application to simple data encryption. *IEEE Transactions on Computers*, 55(10):1300–1305, October 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1683760.

Reddy:2002:AAM

[RKZD02] Prakash Reddy, Venky Krishnan, Kan Zhang, and Devaraj Das. Authentication and authorization of mobile clients in public data networks. *Lecture Notes in Computer Science*, 2437:115–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2437/24370115.htm; http://link.springer.de/link/service/series/0558/papers/2437/24370115.pdf.

Riedl:2002:FSH

[RM02] Reinhard Riedl and Nico Maibaum. FASME — from Smartcards to holistic IT-architectures for interstate e-government. *Lecture Notes in Computer Science*, 2456: 173–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2456/24560173.htm; http://link.springer.de/link/service/series/0558/papers/2456/24560173.pdf.

Roy:2004:FSE

[RM04] Bimal Roy and Willi Meier, editors. *Fast Software Encryption: 11th International Workshop, FSE 2004: Delhi, India, February 5–7, 2004: Revised Papers*, volume 3017 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22171-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://link.springer-ny.com/link/service/series/0558/tocs/t3017.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3017; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b98177.

Ruiz:2001:SPS

[RMCG01] Antonio Ruiz, Gregorio Martínez, Oscar Cánovas, and Antonio F. Gómez. SPEED protocol: Smartcard-based payment with encrypted electronic delivery. *Lecture Notes in Computer Science*, 2200: 446–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2200/22000446.htm; http://link.springer-ny.com/link/service/series/0558/papers/2200/22000446.pdf.

Reyhani-Masoleh:2003:LCS

[RMH03a] Arash Reyhani-Masoleh and M. Anwar Hasan. Low complexity sequential normal basis multipliers over GF(2^m). In Bajard and Schulte [BS03], pages 188–195. ISBN 0-7695-1894-X. ISSN 1063-6889. LCCN ???? URL http://www.acsel-lab.com/arithmetic/arith16/papers/ARITH16_Reyhani-Masoleh.pdf. IEEE order no. PR01894.

Reyhani-Masoleh:2003:LCB

[RMH03b] Arash Reyhani-Masoleh and M. Anwar Hasan. On low complexity bit parallel polynomial basis multipliers. In Walter et al. [WKP03], pages 189–202. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Reyhani-Masoleh:2004:TFT

[RMH04] Arash Reyhani-Masoleh and M. Anwar Hasan. Towards fault-tolerant cryptographic computations over finite fields. *ACM Transactions on Embedded Computing Systems*, 3(3):593–613, August 2004. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Rahaman:2008:CTB

[RMPJ08] H. Rahaman, J. Mathew, D. K. Pradhan, and A. M. Jabir. C-testable bit parallel multipliers over GF(2^m). *ACM Transactions on Design Automation of Electronic Systems*, 13(1):5:1–5:??, January 2008. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Ryabko:2005:NTA

[RMS05] B. Y. Ryabko, V. A. Monarev, and Y. I. Shokin. A new type of attack on block ciphers. *Problems of Information Transmission*, 41(4):385–394, ???? 2005. CODEN PRITA9. ISSN 0032-9460 (print), 1608-3253 (electronic).

Ryutov:2000:RESa

[RN00a] Tatyana Ryutov and Clifford Neuman. Representation and evaluation of security policies. *Operating Systems Review*, 34(2):34, April 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Ryutov:2000:RESb

[RN00b] Tatyana Ryutov and Clifford Neuman. Representation and evaluation of security policies (poster session). *Operating Systems Review*, 34(2):41, April 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Robinson:2002:LLE

[Rob02] Andrew Robinson. *Lost languages: the enigma of the world's undeciphered scripts*. McGraw-Hill, New York, NY, USA, 2002. ISBN 0-07-135743-2 (hardcover). 352 pp. LCCN P211 .R59 2002. URL http://www.

loc.gov/catdir/bios/mh041/2001051412.html; http://www.loc.gov/catdir/description/mh021/2001051412.html; http://www.loc.gov/catdir/toc/fy022/2001051412.html.

Robinson:2009:LLE

[Rob09] Andrew Robinson. *Lost languages: the enigma of the world's undeciphered scripts*. Thames and Hudson, London, UK, 2009. ISBN 0-500-51453-4 (hardcover), 0-500-28816-X (paperback). 352 pp. LCCN CN120 .R63 2009.

Rosen:2000:NRC

[Ros00a] Alon Rosen. A note on the round-complexity of concurrent zero-knowledge. In Bellare [Bel00], pages 451–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800451.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800451.pdf.

Rosenblatt:2000:CBE

[Ros00b] A. Rosenblatt. *The code book: the evolution of secrecy from Mary Queen of Scots to quantum cryptography* [books]. *IEEE Spectrum*, 37(10):10–14, October 2000. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Ross:2004:TCN

[Ros04] P. E. Ross. 10 tech companies for the next 10 years. *IEEE Spectrum*, 41(11):52, November 2004. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Rosen:2006:CZK

[Ros06a] Alon Rosen. *Concurrent Zero-Knowledge*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-642-06949-5, 3-540-32939-0 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xiii + 184 pp. LCCN QA76.9.A25 R657 2006. URL http://www.springerlink.com/content/uu1171. With Additional Background by Oded Goldreich.

Rosenberg:2006:RAS

[Ros06b] Beth Rosenberg, editor. *RFID: applications, security, and privacy*. Addison-Wesley, Reading, MA, USA, 2006. ISBN 0-321-29096-8. li + 555 pp. LCCN TS160 .G37 2005. URL http://www.loc.gov/catdir/toc/ecip059/2005006610.html.

Rosenblum:2007:WAC

[Ros07] David Rosenblum. What anyone can know: The privacy risks of social networking sites. *IEEE Security & Privacy*, 5(3):40–49, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Roth:2001:RSC

[Rot01] Volker Roth. On the robustness of some cryptographic protocols for mobile agent protection. *Lecture Notes in Computer Science*, 2240:1–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2240/22400001.htm; http://link.springer-ny.com/link/service/series/0558/papers/2240/22400001.pdf`.

Roth:2002:JSA

[Rot02a] Volker Roth. Java security architecture and extensions. *Dr. Dobb's Journal of Software Tools*, 27(4):34, 36–38, April 2002. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ftp/2002/2002_04/jca.txt; http://www.ddj.com/ftp/2002/2002_04/jca.zip`.

Rothe:2002:SFC

[Rot02b] Jörg Rothe. Some facets of complexity theory and cryptography: a five-lecture tutorial. *ACM Computing Surveys*, 34(4):504–549, December 2002. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Rothe:2003:SFC

[Rot03] Jörg Rothe. Some facets of complexity theory and cryptography: a five-lecture tutorial. *ACM Computing Surveys*, 34(4):504–549, December 2003. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Rothe:2005:CTC

[Rot05] Jörg Rothe. *Complexity Theory and Cryptology: an Introduction to Cryptocomplexity*. Texts in theoretical computer science: an EATCS series. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 3-540-22147-6, 3-540-28520-2 (e-book). xi + 478 pp. LCCN QA76.9.A25 R672 2005. URL `http://www.myilibrary.com?id=133022; http://www.springerlink.com/openurl.asp?genre=book\%26isbn=978-3-540-22147-0`.

Rothe:2007:BRB

[Rot07] Jörg Rothe. Book review: *Complexity and Cryptography: An Introduction*, by John Talbot and Dominic Welsh, Cambridge University Press, 2006, 292 pages. *ACM SIGACT News*, 38 (2):16–20, June 2007. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL http://doi.acm.org/10.1145/1272729.1272735. See [TW06a].

Roy:2000:PCI

[Roy00a] Bimal Roy, editor. *Progress in cryptology: INDOCRYPT 2000: First International Conference in Cryptology in India, Calcutta, India, December 10–13, 2000: proceedings*, volume 1977 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-41452-5. LCCN QA267.A1 L43 no.1977.

Roychowdhury:2000:PCJ

[Roy00b] Vwani P. Roychowdhury. *Practical cryptography: July 24–27, 2000, Engineering 819.311*. Los Angeles, CA, USA, 2000. (various) pp.

Roy:2005:ACA

[Roy05] Bimal Roy, editor. *Advances in cryptology: ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4–8, 2005*, volume 3788 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-30684-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 2005. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3788.

Rieffel:2000:IQC

[RP00] Eleanor Rieffel and Wolfgang Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, 32(3):300–335, September 2000. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL http://www.acm.org/pubs/articles/journals/surveys/2000-32-3/p300-rieffel/p300-rieffel.pdf; http://www.acm.org/pubs/citations/journals/surveys/2000-32-3/p300-rieffel/.

Ramzan:2000:RSS

[RR00] Zulfikar Ramzan and Leonid Reyzin. On the round security of symmetric-key cryptographic primitives. In Bellare [Bel00], pages 376–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800376.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800376.pdf.

Reyzin:2002:BTB

[RR02] Leonid Reyzin and Natan Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. *Lecture Notes in Computer Science*, 2384: 144–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840144.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840144.pdf.

Ratner:2003:NGI

[RR03a] Daniel Ratner and Mark Ratner. *Nanotechnology: a gentle introduction to the next big idea*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 2003. ISBN 0-13-101400-5. xiv + 188 pp. LCCN T174.7 .R38 2003.

Ratner:2003:NHS

[RR03b] Daniel Ratner and Mark Ratner. *Nanotechnology and Homeland Security: New Weapons for New Wars*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 2003. ISBN 0-13-145307-6. 176 (est.) pp. LCCN UA927.R38 2004. US$24.95.

Rosenberg:2004:SWS

[RR04] Jonathan B. Rosenberg and David L. Remy. *Securing Web services with WS-Security: demystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption*. SAMS Publishing, Indianapolis, IN, USA, 2004. ISBN 0-672-32651-5 (paperback). xiv + 378 pp. LCCN TK5105.59 .R68 2004.

Rittinghouse:2005:IIM

[RR05] John Rittinghouse and James Ransome. *IM Instant Messaging Security*. Elsevier, Amsterdam, The Netherlands, 2005. ISBN 1-55558-338-5. 432 (est.) pp. LCCN ???? URL http://books.elsevier.com/us/mk/us/subindex.asp?isbn=1555583385.

Rechberger:2008:NRN

[RR08] C. Rechberger and V. Rijmen. New results on NMAC/HMAC when instantiated with popular hash functions. *J.UCS: Journal of Universal Computer Science*, 14(3):347–376, ???? 2008. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_14_3/new_results_on_nmac.

Rechberger:2006:NCW

[RRS06] Christian Rechberger, Vincent Rijmen, and Nicolas Sklavos. The NIST Cryptographic Workshop on Hash Functions. *IEEE Security & Privacy*, 4(1):54–56, January/February 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://ieeexplore.ieee.org/iel5/8013/33481/01588827.pdf; http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=33481&arnumber=1588827; http://www.csrc.nist.gov/pki/HashWorkshop/.

Rivest:2000:RA

[RRY00] Ronald L. Rivest, M. J. B. Robshaw, and Yiqun Lisa Yin. RC6 as the AES. In NIST [NIS00], pages 337–342. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Rosenbaum:2000:SFR

[RS00] René Rosenbaum and Heidrun Schumann. A steganographic framework for reference colour based encoding and cover image selection. *Lecture Notes in Computer Science*, 1975: 30–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750030.htm; http://link.springer-ny.com/link/service/series/0558/papers/1975/19750030.pdf.

Romer:2001:ILA

[RS01] Tanja Römer and Jean-Pierre Seifert. Information leakage attacks against smart card implementations of the elliptic curve digital signature algorithm. *Lecture Notes in Computer Science*, 2140:211–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400211.htm;

http://link.springer-ny.com/link/service/series/0558/papers/2140/21400211.pdf.

Rubin:2002:SAV

[RS02] Karl Rubin and Alice Silverberg. Supersingular Abelian varieties in cryptology. In Yung [Yun02a], pages 336–353. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420336.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420336.pdf.

Rubin:2003:TBC

[RS03] Karl Rubin and Alice Silverberg. Torus-based cryptography. In Boneh [Bon03], pages 349–365. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Riley:2004:HAE

[RS04] Joseph Riley and Michael J. Schulte. A hardware accelerator for elliptic curve cryptography over GF(2^m). *International Journal of Computer Research*, ??(??):??, 2004. ISSN 1535-6698. URL http://mesa.ece.wisc.edu/publications/cp_2004-10.pdf. Special Issue on Cryptographic Hardware and Embedded Systems.

Rao:2005:CHE

[RS05] Josyula R. Rao and Berk Sunar, editors. *Cryptographic Hardware and Embedded Systems — CHES 2005: 7th International Workshop, Edinburgh, UK, August 29–September 1, 2005. Proceedings*, volume 3659 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-28474-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3659.

Rubin:2008:CFF

[RS08] K. Rubin and A. Silverberg. Compression in finite fields and torus-based cryptography. *SIAM Journal on Computing*, 37(5):1401–1428, ???? 2008. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

RSA:2000:PKC

[RSA00a] RSA. Public-key cryptography standards. World-Wide Web site., 2000. URL http://www.rsasecurity.com/rsalabs/pkcs/.

RSA:2000:PVCa

[RSA00b] RSA Laboratories. *PKCS #10 v1.7: Certification Request Syntax Standard*. RSA Data Security, Inc., Redwood City, CA, USA, May 26, 2000. 10 pp. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/index.html.

RSA:2000:PCP

[RSA00c] RSA Laboratories. *PKCS #15: Conformance Profile Specification*. RSA Data Security, Inc., Redwood City, CA, USA, August 1, 2000. 8 pp. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html.

RSA:2000:PVCb

[RSA00d] RSA Laboratories. *PKCS #15 v1.1: Cryptographic Token Information Syntax Standard*. RSA Data Security, Inc., Redwood City, CA, USA, June 6, 2000. 81 pp. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html.

RSA:2000:PVS

[RSA00e] RSA Laboratories. *PKCS #9 v2.0: Selected Object Classes and Attribute Types*. RSA Data Security, Inc., Redwood City, CA, USA, February 25, 2000. 34 pp. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-9/index.html.

RSA:2001:PVC

[RSA01] RSA Laboratories. *PKCS #11 v2.11: Cryptographic Token Interface Standard*. RSA Data Security, Inc., Redwood City, CA, USA, November 1, 2001. 374 pp. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html.

RSA:2002:PVR

[RSA02] RSA Laboratories. *PKCS #1 v2.1: RSA Cryptography Standard*. RSA Data Security, Inc., Redwood City, CA, USA, June 14, 2002. 61 pp. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html.

Rivest:2003:TAL

[RSA03a] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. 2002 Turing

Award Lecture. World-Wide Web document., June 7, 2003. URL http://www.acm.org/awards/turing_citations/rivest-shamir-adleman.html. Collection of three slide presentations: "Pre RSA Days" (Adleman), "Early RSA Days" (Rivest), "Turing Lecture on Cryptology: A Status Report" (Shamir).

RSA:2003:PEC

[RSA03b] RSA Laboratories. *PKCS #13: Elliptic Curve Cryptography Standard*. RSA Data Security, Inc., Redwood City, CA, USA, 2003. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-13/index.html. Still under development.

Rousseau:2009:CCP

[RSA09a] Christiane Rousseau and Yvan Saint-Aubin. La cryptographie à cle publique: le code RSA (1978). In *Mathématiques et Technologie* [RSA09b], pages 213–244. ISBN 0-387-69213-4. LCCN ???? URL http://d-nb.info/997902213/34; http://nbn-resolving.de/urn:nbn:de:1111-20091103138; http://www.springerlink.com/content/r61844.

Rousseau:2009:MT

[RSA09b] Christiane Rousseau and Yvan Saint-Aubin, editors. *Mathématiques et Technologie*. Springer Undergraduate Texts in Mathematics and Technology. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 0-387-69213-4. ???? pp. LCCN ???? URL http://d-nb.info/997902213/34; http://nbn-resolving.de/urn:nbn:de:1111-20091103138; http://www.springerlink.com/content/r61844.

Rukhin:2001:STS

[RSN+01] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo. *A Statistical Test Suite For Random and Pseudorandom Number Generators for Cryptographic Applications*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, April 2001. xi + 153 pp. URL http://csrc.nist.gov/rng/rng2.html; http://csrc.nist.gov/rng/SP800-22b.pdf; http://csrc.nist.gov/rng/sts-1.5.tar; http://csrc.nist.gov/rng/sts.data.tar; http://csrc.nist.gov/rng/StsGui.zip; http://www.cs.sunysb.edu/~algorith/implement/rng/distrib/SP800-22b.pdf. NIST

Special Publication 800-22, with revisions dated May 15, 2001.

Rogers:2005:MPH

[RSP05] Brian Rogers, Yan Solihin, and Milos Prvulovic. Memory predecryption: hiding the latency overhead of memory encryption. *ACM SIGARCH Computer Architecture News*, 33(1):27–33, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Rouvroy:2003:EUF

[RSQL03] G. Rouvroy, F.-X. Standaert, J.-J. Quisquater, and J.-D. Legat. Efficient uses of FPGAs for implementations of DES and its experimental linear cryptanalysis. *IEEE Transactions on Computers*, 52(4):473–482, April 2003. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1190588.

Ryabko:2004:NTR

[RSS04] B. Ya. Ryabko, V. S. Stognienko, and Y. I. Shokin. A new test for randomness and its application to some cryptographic problems. *Journal of Statistical Planning and Inference*, 123(2):365–376, July 1, 2004. CODEN JSPIDN. ISSN 0378-3758 (print), 1873-1171 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0378375803001496.

Rivest:2001:HLS

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. *Lecture Notes in Computer Science*, 2248:552–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480552.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480552.pdf.

Rubin:2000:KVL

[Rub00] Aviel D. Rubin. Kerberos versus the Leighton-Micali protocol. *Dr. Dobb's Journal of Software Tools*, 25(11):21–22, 24, 26, November 2000. CODEN DDJOEB. ISSN 1044-789X.

Rubin:2001:SCR

[Rub01] Avi Rubin. Security considerations for remote electronic voting over the Internet. *;login: the USENIX Association newsletter*, 26(1):??, February 2001. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/2001-02/pdfs/rubin.pdf.

Rugg:2004:CMV

[Rug04] Gordon Rugg. Cryptography: The mystery of the Voynich Manuscript. *Scientific American*, 291(1): 104–109, July 2004. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v291/n1/pdf/scientificamerican0704-104.pdf.

Rupp:2009:CAC

[Rup09] Andy Rupp. *Computational aspects of cryptography and cryptanalysis*, volume 6 of *IT-Security*. Europäischer Universitätsverlag, Berlin, Germany, 2009. ISBN 3-89966-337-3. xviii + 245 pp. LCCN ????

Raghavan:2009:SPC

[RVS09] Barath Raghavan, Patric Verkaik, and Alex C. Snoeren. Secure and policy-compliant source routing. *IEEE/ACM Transactions on Networking*, 17(3):764–777, June 2009. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Russell:2002:HFU

[RW02] Alexander Russell and Hong Wang. How to fool an unbounded adversary with a short key. *Lecture Notes in Computer Science*, 2332: 133–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320133.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320133.pdf.

Renner:2003:NBS

[RW03a] Renato Renner and Stefan Wolf. New bounds in secret-key agreement: The gap between formation and secrecy extraction. *Lecture Notes in Computer Science*, 2656: 562–577, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_35.pdf.

Renner:2003:UAP

[RW03b] Renato Renner and Stefan Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. In Boneh [Bon03], pages 78–95. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&

issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Ramaswamy:2007:HSP

[RW07] Ramaswamy Ramaswamy and Tilman Wolf. High-speed prefix-preserving IP address anonymization for passive measurement systems. *IEEE/ACM Transactions on Networking*, 15 (1):26–39, February 2007. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Schmalz:2003:MDI

[S+03] Mark S. Schmalz et al., editors. *Mathematics of data/image coding, compression, and encryption V, with applications: 9–10 July 2002, Seattle, Washington, USA*, volume 4793 of *SPIE proceedings series*. SPIE, Bellingham, Wash., USA, 2003. ISBN 0-8194-4560-6. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TA1637 .M382 2003; TA1637 .M38 2002; TA1637 .M38 2003; TA1637 .M38 2003eb; TA1637; TS510 .S63; Internet. URL http://link.spie.org/PSISDG/4793/1; http://uclibs.org/PID/39661.

Saini:2002:JMD

[SA02] S. P. Saini and F. Ahmad. Java model of DSA (Digital Signature Algorithm). *IETE Technical Review*, 19 (4):189–194, 2002. CODEN ITREEI. ISSN 0256-4602.

Saeednia:2000:HMB

[Sae00] Shahrokh Saeednia. How to maintain both privacy and authentication in digital libraries. *International Journal on Digital Libraries*, 2(4):251–258, May 2000. CODEN ???? ISSN 1432-1300 (print), 1432-5012 (electronic). URL https://link.springer.com/article/10.1007/PL00021469.

Saeednia:2002:IBS

[Sae02] Shahrokh Saeednia. An identity-based society oriented signature scheme with anonymous signers. *Information Processing Letters*, 83(6):295–299, September 30, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sakamura:2001:GEI

[Sak01] Ken Sakamura. Guest editor's introduction: Radio frequency identification and noncontact smart cards. *IEEE Micro*, 21(6): 4–6, November/December 2001. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://dlib.computer.org/mi/books/mi2001/m6004abs.htm; http://dlib.computer.

org/mi/books/mi2001/pdf/m6004.pdf.

Sale:2000:CGL

[Sal00a] Anthony E. Sale. Colossus and the German Lorenz cipher — code breaking in WW II. *Lecture Notes in Computer Science*, 1807: 417–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070417.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070417.pdf.

Sale:2000:CBP

[Sal00b] Anthony E. Sale. The Colossus of Bletchley Park: the German cipher system. In Rojas and Hashagen [RH00], pages 351–364. ISBN 0-262-18197-5 (hardcover), 0-585-35535-5 (electronic). LCCN QA76.17 .F57 2000.

Sale:2001:GRT

[Sal01a] Tony Sale. General report on Tunny: The Newmanry history. Technical report, March 2001. URL http://www.codesandciphers.org.uk/documents/newman/newman.pdf.

Salus:2001:CA

[Sal01b] Peter Salus. 2001: a communications anniversary, 2001. URL http://db.usenix.org/publications/library/proceedings/lisa2001/tech/. Unpublished invited talk, LISA 2001: 15th Systems Administration Conference, December 2–7, 2001, Town and Country Resort Hotel, San Diego, CA.

Salomon:2003:DPS

[Sal03a] David Salomon. *Data Privacy and Security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 0-387-00311-8. xiv + 465 pp. LCCN QA76.9.A25 S265 2003. US$59.95. URL http://www.booksbydavidsalomon.com/.

Salus:2003:BRBb

[Sal03b] Peter H. Salus. Book reviews: The bookworm: Reviews of Pavol Cerven's *Crackproof Your Software* and of Jenness and Cozens's *Extending and Embedding Perl*. *;login: the USENIX Association newsletter*, 28 (2):??, April 2003. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/2003-04/openpdfs/bookreviews.pdf.

Sale:2005:RCB

[Sal05a] Anthony E. Sale. The rebuilding of Colossus at Bletchley Park. *IEEE An-*

nals of the History of Computing, 27(3):61–69, July/September 2005. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic).

Sallee:2005:MBM

[Sal05b] Phil Sallee. Model-based methods for steganography and steganalysis. *International Journal of Image and Graphics (IJIG)*, 5(1):167–??, January 2005. CODEN ???? ISSN 0219-4678.

Salomon:2005:CDC

[Sal05c] David Salomon. *Coding for data and computer communications*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 0-387-21245-0. xv + 548 pp. LCCN TK5102.94 .S35 2005. URL `http://www.DavidSalomon.name/Codes/Codes.html`; `http://www.ecs.csun.edu/~dsalomon/`.

Salomon:2005:FCS

[Sal05d] David Salomon. *Foundations of computer security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 1-84628-193-8, 1-84628-341-8. xxi + 368 pp. LCCN QA76.9.A25 S2656 2005. URL `http://www.springer.com/sgw/cda/frontpage/0,11855,4-40007-22-65173048-0,00.html`; `http://www.springer.com/sgw/cda/pageitems/document/cda_downloaddocument/0,11855,0-0-45-166687-p65173048,00.pdf`; `http://www.springer.com/sgw/cda/pageitems/document/cda_downloaddocument/0,11855,0-0-45-166688-p65173048,00.pdf`; `http://www.springer.com/sgw/cda/pageitems/document/cda_downloaddocument/0,11855,0-0-45-166689-p65173048,00.pdf`.

Salomon:2007:DCC

[Sal07] David Salomon. *Data Compression: The Complete Reference*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 1-84628-602-6. xxv + 1092 pp. LCCN ???? With contributions by Giovanni Motta and David Bryant.

Sale:20xx:CRP

[Salxx] Tony Sale. The Colossus rebuild project. World-Wide Web site., 20xx. URL `http://www.codesandciphers.org.uk/lorenz/rebuild.htm`.

Samid:2001:ESR

[Sam01] Gideon Samid. Encryption sticks (randomats). *Lecture Notes in Computer Science*, 2229:150–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290150.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290150.pdf.

Samtani:2009:WTO

[Sam09] Rajan Samtani. Web technologies: Ongoing innovation in digital watermarking. *Computer*, 42(3):92–94, March 2009. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Santini:2005:WSI

[San05] Simone Santini. We are sorry to inform you .... *Computer*, 38(12):128, 126–127, December 2005. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Sarkar:2002:FCM

[Sar02] Palash Sarkar. The filter-combiner model for memoryless synchronous stream ciphers. In Yung [Yun02a], pages 533–548. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420533.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420533.pdf.

Sasse:2007:REB

[Sas07] M. Angela Sasse. Red-eye blink, bendy shuffle, and the yuck factor: a user experience of biometric airport systems. *IEEE Security & Privacy*, 5(3):78–81, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Satoh:2006:DPI

[Sat06] Takakazu Satoh. On degrees of polynomial interpolations related to elliptic curve cryptography. In Ytrehus [Ytr06], pages 155–163. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Savelli:2004:NDC

[Sav04] A. Savelli. On numerically decipherable codes and their homophonic partitions. *Information Processing Letters*, 90(3):103–108, May 16, 2004. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Savage:2005:IPWa

[Sav05a] P. R. Savage. Invention: Patent watch. *IEEE Spectrum*, 42(1):70–71, January 2005. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Savage:2005:IPWb

[Sav05b] P. R. Savage. Inventions: Patent watch. *IEEE Spectrum*, 42(3):64, March 2005. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Soto:2000:RTA

[SB00] Juan Soto and Lawrence E. Bassham. Randomness testing of the Advanced Encryption Standard finalist candidates. NIST internal report 6483, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, April 2000. URL http://csrc.nist.gov/rng/aes-report-final.doc.

Shacham:2001:ISH

[SB01] Hovav Shacham and Dan Boneh. Improving SSL handshake performance via batching. *Lecture Notes in Computer Science*, 2020: 28–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200028.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200028.pdf.

Scott:2004:CP

[SB04] Michael Scott and Paulo S. L. M. Barreto. Compressed pairings. In Franklin [Fra04], pages 140–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Stoklosa:2005:CIC

[SB05] Janusz Stoklosa and Jaroslaw Bubicz. Compound inversive congruential generator as a source of keys for stream ciphers. In Hamid R. Arabnia, Liwen He, and Youngsong Mun, editors, *Proceedings of the 2005 International Conference on Security and Management, SAM '05: Las Vegas, Nevada, USA, June 20-23, 2005*, pages 473–478. CSREA Press, Las Vegas, NV, USA, 2005. ISBN 1-932415-82-3. LCCN TK5105.59 .I57 2005.

Stallings:2007:CSP

[SB07] William Stallings and Lawrie Brown. *Computer Security: Principles and Practice*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 2007. ISBN 0-13-600424-5. ???? pp. LCCN ????

Sherwood:2005:MTR

[SBB05] Rob Sherwood, Bobby Bhattacharjee, and Ryan Braud. Misbehaving TCP receivers can cause Internet-wide congestion collapse. In Meadows and Syverson [MS05b], pages 383–392. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Steiner:2001:SPB

[SBEW01] Michael Steiner, Peter Buhler, Thomas Eirich, and Michael Waidner. Secure password-based cipher suite for TLS. *ACM Transactions on Information and System Security*, 4(2):134–157, May 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Smeraldi:2002:SVF

[SBG02] Fabrizio Smeraldi, Josef Bigun, and Wulfram Gerstner. Support vector features and the role of dimensionality in face authentication. *Lecture Notes in Computer Science*, 2388:249–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2388/23880249.htm; http://link.springer-ny.com/link/service/series/0558/papers/2388/23880249.pdf.

Shehab:2005:SCM

[SBG05] Mohamed Shehab, Elisa Bertino, and Arif Ghafoor. Secure collaboration in mediator-free environments. In Meadows and Syverson [MS05b], pages 58–67. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Shehab:2007:WSD

[SBG07] Mohamed Shehab, Kamal Bhattacharya, and Arif Ghafoor. Web services discovery in secure collaboration environments. *ACM Transactions on Internet Technology (TOIT)*, 8(1): 5:1–5:??, November 2007. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Shaikh:2009:SAU

[SBS09] Siraj A. Shaikh, Vicky J. Bush, and Steve A. Schneider. Specifying authentication using signal events in CSP. *Computers & Security*, 28(5):310–324, July 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808000953.

Steinfeld:2002:NSA

[SBZ02] Ron Steinfeld, Joonsang Baek, and Yuliang Zheng. On the necessity of strong assumptions for the security of a class of asymmetric encryption schemes. *Lecture Notes in Computer Science*, 2384:241–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840241.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840241.pdf.

Seredynski:2004:CAC

[SBZ04] Franciszek Seredynski, Pascal Bouvry, and Albert Y. Zomaya. Cellular automata computations and secret key cryptography. *Parallel Computing*, 30(5–6):753–766, May/June 2004. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Syverson:2001:LAP

[SC01] Paul Syverson and Iliano Cervesato. The logic of authentication protocols. *Lecture Notes in Computer Science*, 2171:63–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2171/21710063.htm; http://link.springer-ny.com/link/service/series/0558/papers/2171/21710063.pdf.

Shen:2002:NDW

[SC02a] Kuan-Ting Shen and Ling-Hwei Chen. A new digital watermarking technique for video. *Lecture Notes in Computer Science*, 2314:269–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2314/23140269.htm; http://link.springer-ny.com/link/service/series/0558/papers/2314/23140269.pdf.

Stoll:2002:MMC

[SC02b] Michael Stoll and John E. Cremona. Minimal models for 2-coverings of elliptic curves. *LMS Journal of Computation and Mathematics*, 5:220–??, 2002. CODEN ???? ISSN 1461-1570. URL http://www.lms.ac.uk/jcm/5/lms2002-013/.

Sun:2002:WDC

[SC02c] Hung-Min Sun and Bor-Liang Chen. Weighted decomposition construction for perfect secret sharing schemes. *Computers and Mathematics with Applications*, 43(6–7):877–887, March/April 2002. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122101003285.

Shao:2005:NEV

[SC05a] Jun Shao and Zhenfu Cao. A new efficient (*tn*) verifiable multi-secret sharing (VMSS) based on YCH scheme. *Applied Mathematics and Computation*, 168(1):135–140, September 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300304005922.

Stephanides:2005:GAK

[SC05b] George Stephanides and Nicolae Constantinescu. The GN-authenticated key agreement. *Applied Mathematics and Computation*, 170(1):531–544, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Sun:2005:IPK

[SC05c] Da-Zhi Sun and Zhen-Fu Cao. Improved public key authentication scheme for non-repudiation. *Applied Mathematics and Computation*, 168(2):927–932, September 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Siegelin:2001:SCD

[SCF01] C. Siegelin, L. Castillo, and U. Finger. Smart Cards: Distributed computing with $5 devices. *Parallel Processing Letters*, 11(1):57–??, March 2001. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Schmalz:2000:MAD

[Sch00a] Mark S. Schmalz, editor. *Mathematics and applications of data/image coding, compression, and encryption III: 2 August 2000, San Diego, USA*, volume 4122 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 2000. ISBN 0-8194-3767-0. LCCN TA1637 .M378 2000. Earlier conferences have title: Mathematics of data/image coding, compression, and encryption.

Schneier:2000:AAR

[Sch00b] Bruce Schneier. Abstracts of AES-related papers from the Fast Software Encryption Workshop (FSE) 2000. In NIST [NIS00], pages 9–10. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-

2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Schneier:2000:IRS

[Sch00c] Bruce Schneier. Inside risks: semantic network attacks. *Communications of the Association for Computing Machinery*, 43(12):168, December 2000. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/2000-43-12/p168-schneier/. See letters [CZB+01, CTBA+01].

Schneier:2000:SLD

[Sch00d] Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley and Sons, Inc., New York, NY, USA, 2000. ISBN 0-471-25311-1. xv + 412 pp. LCCN QA76.9.A25 S352 2000. US$29.99.

Schneier:2000:SRF

[Sch00e] Bruce Schneier. Security research and the future. *Dr. Dobb's Journal of Software Tools*, 25(12 (supplement)): 33–35, December 2000. CODEN DDJOEB. ISSN 1044-789X.

Scharinger:2001:ASK

[Sch01a] Josef Scharinger. Application of signed Kolmogorov hashes to provide integrity and authenticity in Web-based software distribution. *Lecture Notes in Computer Science*, 2178:257–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2178/21780257.htm; http://link.springer-ny.com/link/service/series/0558/papers/2178/21780257.pdf.

Schindler:2001:TAA

[Sch01b] Werner Schindler. A timing attack against RSA with the Chinese Remainder Theorem. *Lecture Notes in Computer Science*, 1965:109–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650109.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650109.pdf.

Schmalz:2001:MDI

[Sch01c] Mark S. Schmalz, editor. *Mathematics of data/image coding, compression, and encryption IV, with* *applications: 30–31 July, 2001, San Diego, [California] USA*, volume 4475 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 2001. ISBN 0-8194-4189-9. LCCN TA1637 .M375 2001. Previous conference has title: Mathematics and applications of data/image coding, compression, and encryption III.

Schneier:2001:FSE

[Sch01d] Bruce Schneier, editor. *Fast software encryption: 7th International Workshop, FSE 2000, New York, NY, USA, April 10–12, 2000: Proceedings*, volume 1978 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-41728-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no. 1978. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1978.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1978.

Schnorr:2001:SGH

[Sch01e] C. P. Schnorr. Small generic hardcore subsets for the discrete logarithm: Short secret DL-keys. *Information Processing Letters*, 79 (2):93–98, June 30, 2001. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.nl/gej-ng/10/23/20/80/31/31/abstract.html; http://www.elsevier.nl/gej-ng/10/23/20/80/31/31/article.pdf.

Schnorr:2001:SDE

[Sch01f] Claus Peter Schnorr. Security of DL-encryption and signatures against generic attacks—a survey. In *Public-key cryptography and computational number theory (Warsaw, 2000)*, pages 257–282. Walter de Gruyter, New York, NY, USA, 2001.

Schultz:2002:GBC

[Sch02] E. Eugene Schultz. The gap between cryptography and information security. *Computers & Security*, 21(8):674–676, November 2002. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404802008015.

Schneier:2003:BFT

[Sch03] Bruce Schneier. *Beyond fear: thinking sensibly about security in an uncertain world*. Copernicus (a division of Springer-Verlag New

York, Inc.), 175 Fifth Avenue, New York, NY 10010, USA, 2003. ISBN 0-387-02620-7. 295 pp. LCCN HV6432 .S36 2003.

Schmalz:2004:MDIa

[Sch04a] Mark S. Schmalz, editor. *Mathematics of data/image coding, compression, and encryption VI, with applications: 5 and 7 August 2003, San Diego, California, USA*, volume 5208 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 2004. ISBN 0-8194-5081-2. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TA1637 .M375 2005.

Schmalz:2004:MDIb

[Sch04b] Mark S. Schmalz, editor. *Mathematics of data/ image coding, compression, and encryption VII, with applications: 4–5 August, 2004, Denver, Colorado, USA*, volume 5561 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 2004. ISBN 0-8194-5499-0. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TA1637 .M375 2004. URL `http://uclibs.org/PID/57292`.

Schneier:2004:SA

[Sch04c] Bruce Schneier. Sensible authentication. *ACM Queue: Tomorrow's Computing Today*, 1(10):74–78, February 2004. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Schultz:2004:GBC

[Sch04d] E. Eugene Schultz. The gap between cryptography and information security: has it narrowed? *Computers & Security*, 23(7):531–532, October 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404804002287`.

Schmalz:2005:MDI

[Sch05a] Mark S. Schmalz, editor. *Mathematics of data/image coding, compression, and encryption VIII, with applications: 1–3 August, 2005, San Diego, California, USA*, volume 5915 of *Proceedings of SPIE*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 2005. ISBN 0-8194-5920-8. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TA1637 .M375 2005; TA1637; Internet. URL `http://uclibs.org/PID/98054`.

Schneier:2005:AE

[Sch05b] B. Schneier. Authentication and expiration. *IEEE Security & Privacy*, 3(1):88, January/February 2005. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://ieeexplore.ieee.org/iel5/8013/30310/01392710.pdf`; `http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=30310&arnumber=1392710&count=17&index=16`.

Schneier:2005:TFA

[Sch05c] Bruce Schneier. Two-factor authentication: too little, too late. *Communications of the Association for Computing Machinery*, 48(4):136, April 2005. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Schramm:2006:AMS

[Sch06a] Kai Schramm. *Advanced Methods in Side Channel Cryptanalysis*. Europäischer Universitätsverlag, Bochum, Germany, 2006. ISBN 3-89966-187-7. 170 pp. LCCN ???? EUR 22.90. URL `http://verlag.rub.de/g9783899661873.html`.

Schroeder:2006:NTS

[Sch06b] Manfred Robert Schroeder. *Number Theory in Science and Communication: With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity*, volume 7 of *Springer Series in Information Sciences*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., fourth edition, 2006. ISBN 3-540-26598-8, 3-540-26596-1. ISSN 0720-678X. xxvi + 367 pp. LCCN QA241.

Schneier:2007:NCS

[Sch07] Bruce Schneier. Nonsecurity considerations in security decisions. *IEEE Security & Privacy*, 5(3):88, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Schneier:2008:SS

[Sch08] Bruce Schneier. *Schneier on Security*. John Wiley and Sons, Inc., New York, NY, USA, 2008. ISBN 0-470-39535-4. viii + 328 pp. LCCN QA76.9.A25.S35145 2008.

Schmeh:2009:VBF

[Sch09] Klaus Schmeh. *Versteckte Botschaften: die faszinierende Geschichte der Steganografie. (German) [Hidden Messages. The Fascinating Story of Steganography]*. Telepolis. Heise, Hannover, Germany, 2009. ISBN 3-936931-54-2 (paperback). xi + 234 pp. LCCN

???? SFR 32.00; EUR 18.00.

Su:2005:IBT

[SCL05] Pin-Chang Su, Henry Ker-Chang Chang, and Erl-Huei Lu. ID-based threshold digital signature schemes on the elliptic curve discrete logarithm problem. *Applied Mathematics and Computation*, 164(3):757–772, May 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Scott:2004:CIB

[Sco04] Michael Scott. Cryptanalysis of an ID-based password authentication scheme using Smart Cards and fingerprints. *Operating Systems Review*, 38(2):73–75, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Screamer:2001:MDR

[Scr01] Beale Screamer. Microsoft's digital rights management scheme — technical details. Report, Microsoft Corporation, Redmond, WA, USA, October 20, 2001. URL `http://cryptome.org/ms-drm.htm`.

Shen:2005:NCB

[SCS05a] Victor R. L. Shen, Tzer-Shyong Chen, and Kai-Quan Shai. A novel cryptosystem based on grey system theory and genetic algorithm. *Applied Mathematics and Computation*, 170(2):1290–1302, November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Sun:2005:CCL

[SCS05b] Da-Zhi Sun, Zhen-Fu Cao, and Yu Sun. Comment: cryptanalysis of Lee–Hwang–Li's key authentication scheme. *Applied Mathematics and Computation*, 164(3):675–678, May 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). See [ZK05].

Sun:2005:RNK

[SCS05c] Da-Zhi Sun, Zhen-Fu Cao, and Yu Sun. Remarks on a new key authentication scheme based on discrete logarithms. *Applied Mathematics and Computation*, 167(1):572–575, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Sebe:2001:OIW

[SDF01] Francesc Sebé and Josep Domingo-Ferrer. Oblivious image watermarking robust against scaling and geometric distortions. *Lecture Notes in Computer Science*,

2200:420–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2200/22000420.htm; http://link.springer-ny.com/link/service/series/0558/papers/2200/22000420.pdf.

Sebe:2000:SDI

[SDFH00] Francesc Sebé, Josep Domingo-Ferrer, and Jordi Herrera. Spatial-domain image watermarking robust against compression, filtering, cropping and scaling. *Lecture Notes in Computer Science*, 1975:44–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750044.htm; http://link.springer-ny.com/link/service/series/0558/papers/1975/19750044.pdf.

Smith:2006:CNS

[SDMN06] Adam Smith, Cynthia Dwork, Frank McSherry, and Kobbi Nissim. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference (TCC) 2006 conference proceedings*, page ?? ????, ????, 2006.

Smith:2001:ADB

[SE01] Michael Smith and Ralph Erskine, editors. *Action This Day: Bletchley Park from the breaking of the Enigma Code to the birth of the modern computer*. Bantam Doubleday Dell Publishing Group Inc., 666 Fifth Avenue, New York, NY 10130, USA, 2001. ISBN 0-593-04910-1. xv + 543 pp. LCCN D810.C88 A28 2001. UK£25.00. URL http://frode.home.cern.ch/frode/crypto/ActionContents.html.

Spiekermann:2009:ACR

[SE09] Sarah Spiekermann and Sergei Evdokimov. Authentication: Critical RFID privacy-enhancing technologies. *IEEE Security & Privacy*, 7(2):56–62, March/April 2009. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Seacord:2005:SCC

[Sea05] Robert C. Seacord. *Secure coding in C and C++*. Addison-Wesley, Reading, MA, USA, 2005. ISBN 0-321-33572-4 (paperback). xxiv + 341 pp. LCCN QA76.9.A25 S368 2005. URL http://www.cert.org/books/secure-coding/; http://www.loc.gov/catdir/toc/ecip0513/2005015012.html.

Seacord:2009:CCS

[Sea09] Robert C. Seacord. *The CERT C secure coding standard*. Addison-Wesley, Reading, MA, USA, 2009. ISBN 0-321-56321-2 (paperback). xxxiii + 682 pp. LCCN QA76.73.C15 S4155 2008.

Seetharaman:2004:BRB

[See04] Priya Seetharaman. Book review: *Beyond Fear—Thinking Sensibly About Security in an Uncertain World*, by Bruce Schneier. *The Computer Journal*, 47 (3):397, May 2004. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/free_pdf/470397.pdf; http://www3.oup.co.uk/computer_journal/hdb/Volume_47/Issue_03/470397.sgm.abs.html.

Smith:2006:SID

[SEF+06] Matthew Smith, Michael Engel, Thomas Friese, Bernd Freisleben, Gregory A. Koenig, and William Yurcik. Security issues in on-demand grid and cluster computing. In Turner et al. [TLC06], pages 24–?? ISBN 0-7695-2585-7. LCCN QA76.9.C58. IEEE Computer Society Order Number P2585.

Seifried:2000:C

[Sei00a] Kurt Seifried. Crypto 101. *Sys Admin: The Journal for UNIX Systems Administrators*, 9(5):16, 20, 22, 24, 26–27, May 2000. CODEN SYADE7. ISSN 1061-2688. URL http://www.samag.com/.

Seifried:2000:PPA

[Sei00b] Kurt Seifried. PAM — Pluggable Authentication Modules. *Sys Admin: The Journal for UNIX Systems Administrators*, 9(9):8, 10, 12, 14, September 2000. CODEN SYADE7. ISSN 1061-2688. URL http://www.samag.com/.

Seifert:2005:ACR

[Sei05] Jean-Pierre Seifert. On authenticated computing and RSA-based authentication. In Meadows and Syverson [MS05b], pages 122–127. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Speed:2001:PIS

[SEK01] Timothy Speed, Juanita Ellis, and Steffano Korper. *The Personal Internet Security Guidebook: Keeping Hackers and Crackers out of Your Home*. Academic Press, New York, NY, USA, 2001. ISBN 0-12-656561-9. xxiv + 202 pp. LCCN ???? US$44.95.

Speed:2002:PIS

[SEK02] Timothy Speed, Juanita Ellis, and Steffano Korper. *The Personal Internet Security Guidebook: Keeping Hackers and Crackers out of Your Home*. The Korper and Ellis e-commerce books series. Academic Press, New York, NY, USA, 2002. ISBN 0-12-656561-9. xxiv + 202 pp. LCCN TK5105.59 .S6423 2002. US$44.95.

Selcuk:2000:BEL

[Sel00] Ali Aydın Selçuk. On bias estimation in linear cryptanalysis. *Lecture Notes in Computer Science*, 1977:52–66, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Semanko:2000:CAA

[Sem00] Michael Semanko. L-collision attacks against randomized MACs. In Bellare [Bel00], pages 216–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800216.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800216.pdf.

Sennewald:2003:ESM

[Sen03] Charles A. Sennewald. *Effective security management*. Butterworth-Heinemann, Boston, MA, USA, 2003. ISBN 0-7506-7454-7. xx + 395 pp. LCCN HV8290 .S46 2003. US$49.95.

Sergienko:2006:QCC

[Ser06] Alexander V. Sergienko, editor. *Quantum communications and cryptography*. Taylor and Francis, Boca Raton, FL, USA, 2006. ISBN 0-8493-3684-8. 232 pp. LCCN TK5102.94 .Q36 2005. URL http://www.loc.gov/catdir/enhancements/fy0648/2005050636-d.html; http://www.loc.gov/catdir/toc/fy0713/2005050636.html.

Sutherland:2008:AVO

[SETB08] Iain Sutherland, Jon Evans, Theodore Tryfonas, and Andrew Blyth. Acquiring volatile operating system data tools and techniques. *Operating Systems Review*, 42(3):65–73, April 2008. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Shumow:2007:PBD

[SF07] Dan Shumow and Niels Ferguson. On the possibility of a back door in the NIST SP800-90 Dual EC Prng. Web slide show., August 21, 2007. URL http://rump2007.cr.yp.to/15-shumow.pdf.

Simka:2006:MTR

[SFDF06] M. Simka, V. Fischer, M. Drutarovsky, and J. Fayolle. Model of a true random number generator aimed at cryptographic application. In *ISCAS 2006: 2006 IEEE International Symposium on Circuits and Systems: Circuits and systems: at crossroads of life and technology: proceedings: May 21–24: Kos International Convention Centre (KICC), Island of Kos, Greece*, pages 5619–5623. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2006. ISBN 0-7803-9390-2. LCCN ???? URL `http://www.ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=11145`. IEEE catalog number 06CH37717C.

Sakr:2007:RCB

[SG07] Ziad Sakr and Nicolas D. Georganas. Robust content-based MPEG-4 XMT scene structure authentication and multimedia content location. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 3(3):18:1–18:??, August 2007. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Sutton:2007:FBF

[SGA07] Michael Sutton, Adam Greene, and Pedram Amini. *Fuzzing: brute force vulnerability discovery*. Addison-Wesley, Reading, MA, USA, 2007. ISBN 0-321-44611-9 (paperback). xxvii + 543 pp. LCCN QA76.9.A25 S89 2007. URL `http://www.loc.gov/catdir/toc/ecip0713/2007011463.html`.

Steinwandt:2001:TDB

[SGB01] Rainer Steinwandt, Willi Geiselmann, and Thomas Beth. A theoretical DPA-based cryptanalysis of the NESSIE candidates FLASH and SFLASH. *Lecture Notes in Computer Science*, 2200:280–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2200/22000280.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2200/22000280.pdf`.

Steinwandt:2000:WHS

[SGGB00] Rainer Steinwandt, Markus Grassl, Willi Geiselmann, and Thomas Beth. Weaknesses in the $\mathrm{SL}_2(\mathbf{F}_{2^n})$ hashing scheme. In Bellare [Bel00], pages 287–299. ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.com/link/service/series/`

0558/bibs/1880/18800287.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800287.pdf.

Steinwandt:2008:GEI

[SGK08] Rainer Steinwandt, Willi Geiselmann, and Çetin Kaya Koç. Guest Editors' introduction to the special section on special-purpose hardware for cryptography and cryptanalysis. *IEEE Transactions on Computers*, 57(11):1441–1442, November 2008. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4633726.

Sauvage:2009:ERF

[SGM09] Laurent Sauvage, Sylvain Guilley, and Yves Mathieu. Electromagnetic radiations of FPGAs: High spatial resolution cartography and attack on a cryptographic module. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 2(1):4:1–4:??, March 2009. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Storer:2009:PSR

[SGMV09] Mark W. Storer, Kevin M. Greenan, Ethan L. Miller, and Kaladhar Voruganti. POTSHARDS — a secure, recoverable, long-term archival storage system. *ACM Transactions on Storage*, 5(2):5:1–5:??, June 2009. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Stone:1998:PCC

[SGPH98] Jonathan Stone, Michael Greenwald, Craig Partridge, and James Hughes. Performance of checksums and CRC's over real data. *IEEE/ACM Transactions on Networking*, 6(5):529–543, October 1998. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL http://www.acm.org/pubs/citations/journals/ton/1998-6-5/p529-stone/.

Sonntag:2000:MAS

[SH00] Michael Sonntag and Rudolf Hörmanseder. Mobile agent security based on payment. *Operating Systems Review*, 34(4):48–55, October 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Shirase:2005:AEC

[SH05] Masaaki Shirase and Yasushi Hibino. An architecture for elliptic curve cryptography computation. *ACM SIGARCH Computer Architecture News*, 33(1):124–133, March 2005. CO-

DEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Seyedzadeh:2011:IEA

[SH11] Seyed Mohammad Seyedzadeh and Yasaman Hashemi. Image encryption algorithm based on Choquet Fuzzy Integral with self-adaptive pseudo-random number generator. In *2011 11th International Conference on Intelligent Systems Design and Applications (ISDA)*, pages 642–647. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6121728.

Shailer:2001:PMT

[Sha01a] David M. Shailer. *The project manager's toolkit: practical checklists for systems development*. Butterworth-Heinemann, Boston, MA, USA, 2001. ISBN 0-7506-5035-4. xiii + 244 pp. LCCN QA76.9.S88 S53 2001. US$39.95.

Shamir:2001:NDC

[Sha01b] A. Shamir. New directions in cryptography. *Lecture Notes in Computer Science*, 2162:159–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620159.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620159.pdf.

Shamir:2001:PSC

[Sha01c] Adi Shamir. Protecting smart cards from passive power analysis with detached power supplies. *Lecture Notes in Computer Science*, 1965:71–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650071.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650071.pdf.

Shao:2001:BVM

[Sha01d] Zuhua Shao. Batch verifying multiple DSA-type digital signatures. *Computer Networks (Amsterdam, Netherlands: 1999)*, 37(3–4):383–389, November 5, 2001. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.elsevier.nl/gej-ng/10/15/22/67/34/35/abstract.html.

Sharp:2001:IKB

[Sha01e] Toby Sharp. An implementation of key-based digital signal steganography. *Lec-*

ture Notes in Computer Science, 2137:13–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370013.htm; http://link.springer-ny.com/link/service/series/0558/papers/2137/21370013.pdf.

Shapiro:2002:CCM

[Sha02] Jonathan S. Shapiro. CPCMS: a configuration management system based on cryptographic names. In USENIX [USE02c], page ?? ISBN 1-880446-01-4. LCCN QA76.8.U65 P765 2002. URL http://www.usenix.org/publications/library/proceedings/usenix02/tech/freenix/shapiro.html.

Shamir:2003:RS

[Sha03a] Adi Shamir. RSA shortcuts. In Joye [Joy03b], page 327. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Shamir:2003:TLC

[Sha03b] Adi Shamir. Turing Lecture on cryptology: a status report. World-Wide Web slide presentation, video, and audio., 2003. URL http://www.acm.org/turingawardlecture/RSA/.

Shao:2003:CIB

[Sha03c] Zuhua Shao. Cryptanalysis of "an identity-based society oriented signature scheme with anonymous signers". *Information Processing Letters*, 86(6):295–298, June 30, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shao:2003:PSS

[Sha03d] Zuhua Shao. Proxy signature schemes based on factoring. *Information Processing Letters*, 85(3):137–143, February 14, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shaltiel:2004:RDE

[Sha04a] Ronen Shaltiel. Recent developments in extractors. In Păun et al. [PRS04], page ?? ISBN 981-238-783-8 (set), 981-238-966-0 (vol. 1), 981-238-965-2 (vol. 2). LCCN QA76 .C878 2004. URL http://www.cs.haifa.ac.il/~ronen/online_papers/online_papers.html; http://www.cs.

haifa.ac.il/~ronen/online_papers/survey.ps.

Shao:2004:IDS

[Sha04b] Zuhua Shao. Improvement of digital signature with message recovery using self-certified public keys and its variants. *Applied Mathematics and Computation*, 159(2):391–399, December 6, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Shao:2005:CXY

[Sha05a] Zuhua Shao. Cryptanalysis of Xia–You group signature scheme. *The Journal of Systems and Software*, 75(1–2): 89–94, February 15, 2005. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Shao:2005:IEP

[Sha05b] Zuhua Shao. Improvement of efficient proxy signature schemes using self-certified public keys. *Applied Mathematics and Computation*, 168(1):222–234, September 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Shao:2005:NKA

[Sha05c] Zuhua Shao. A new key authentication scheme for cryptosystems based on discrete logarithms. *Applied Mathematics and Computation*, 167(1):143–152, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Shao:2005:SMD

[Sha05d] Zuhua Shao. Security of Meta-He digital signature scheme based on factoring and discrete logarithms. *Applied Mathematics and Computation*, 170(2):976–984, November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Hwang:2009:KDB

[sHCP09] Seong seob Hwang, Sungzoon Cho, and Sunghoon Park. Keystroke dynamics-based authentication for mobile devices. *Computers & Security*, 28(1–2):85–93, February/March 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808000965.

Shepherd:2001:CDC

[She01] Simon Shepherd. *Cryptography: diffusing the confusion*, volume 5 of *Communications systems, techniques, and applications series*. Research Studies Press, Philadelphia, PA, USA, 2001. ISBN 0-86380-

270-2. xiv + 152 pp. LCCN QA268.S44 2001.

Sung:2007:CIB

[SHH07] Jaechul Sung, Deukjo Hong, and Seokhie Hong. Cryptanalysis of an involutional block cipher using cellular automata. *Information Processing Letters*, 104(5):183–185, November 30, 2007. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shim:2005:LPG

[Shi05] Kyungah Shim. Off-line password-guessing attacks on the generalized key agreement and password authentication protocol. *Applied Mathematics and Computation*, 169(1):511–515, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Shih:2008:DWS

[Shi08] Frank Y. Shih. *Digital Watermarking and Steganography: Fundamentals and Techniques*. Taylor and Francis, Boca Raton, FL, USA, 2008. ISBN 1-4200-4757-4. 180 pp. LCCN QA76.9.A25 S467 2008. URL `http://www.loc.gov/catdir/enhancements/fy0745/2007034224-d.html`; `http://www.loc.gov/catdir/toc/ecip0725/2007034224.html`.

Sierra:2004:LCC

[SHJR04] José M. Sierra, Julio C. Hernández, Narayana Jayaram, and Arturo Ribagorda. Low computational cost integrity for block ciphers. *Future Generation Computer Systems*, 20(5):857–863, June 15, 2004. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Shimizu:2007:CBE

[SHL07] K. Shimizu, H. P. Hofstee, and J. S. Liberty. Cell Broadband Engine processor vault security architecture. *IBM Journal of Research and Development*, 51(5):521–??, September 2007. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http://www.research.ibm.com/journal/rd/515/shimizu.html`.

Shoup:2000:CTU

[Sho00a] Victor Shoup. A composition theorem for universal one-way hash functions. *Lecture Notes in Computer Science*, 1807:445–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070445.htm`; `http://link.springer-`

ny.com/link/service/series/0558/papers/1807/18070445.pdf.

Shoup:2000:UHF

[Sho00b] Victor Shoup. Using hash functions as a hedge against chosen ciphertext attack. *Lecture Notes in Computer Science*, 1807: 275–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070275.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070275.pdf.

Shoup:2001:OR

[Sho01] Victor Shoup. OAEP reconsidered. In Kilian [Kil01a], pages 239–259. ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139. UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390239.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390239.pdf.

Shoup:2005:ACC

[Sho05a] Victor Shoup, editor. *Advances in cryptology: CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14–18, 2005: proceedings*, volume 3621 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Shoup:2005:CIN

[Sho05b] Victor Shoup. *A computational introduction to number theory and algebra*. Cambridge University Press, Cambridge, UK, 2005. ISBN 0-521-85154-8 (hardcover), 0-521-61725-1 (paperback). xvi + 517 pp. LCCN QA241 .V53 2005.

Shparlinski:1999:NTM

[Shp99] Igor E. Shparlinski. *Number theoretic methods in cryptography: complexity lower bounds*, volume 17 of *Progress in computer science and applied logic*. Birkhäuser Verlag, Basel, Switzerland, 1999. ISBN 3-7643-5888-2 (Basel), 0-8176-5888-2 (Boston). viii + 180 pp. LCCN QA267.7 .S57 1999.

Shparlinski:2001:UDR

[Shp01] Igor E. Shparlinski. On the uniformity of distribution of the RSA pairs. *Mathematics of Computation*, 70(234):801–808, April 2001. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journal-getitem?pii=S0025-5718-00-01274-6; http://www.ams.org/mcom/2001-70-234/S0025-5718-00-01274-6/S0025-5718-00-01274-6.dvi; http://www.ams.org/mcom/2001-70-234/S0025-5718-00-01274-6/S0025-5718-00-01274-6.pdf; http://www.ams.org/mcom/2001-70-234/S0025-5718-00-01274-6/S0025-5718-00-01274-6.ps; http://www.ams.org/mcom/2001-70-234/S0025-5718-00-01274-6/S0025-5718-00-01274-6.tex.

Shparlinski:2002:SMS

[Shp02] Igor E. Shparlinski. Security of most significant bits of g^{x^2}. *Information Processing Letters*, 83(2):109–113, July 31, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shparlinski:2003:CAA

[Shp03] Igor E. Shparlinski. *Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness*, volume 22 of *Progress in computer science and applied logic*. Birkhäuser Verlag, Basel, Switzerland, 2003. ISBN 3-7643-6654-0 , 0-8176-6654-0. viii + 411 pp. LCCN QA267.7 .S55 2003.

Shparlinski:2004:BRR

[Shp04a] Igor Shparlinski. Book review: *RSA and public-key cryptography*. *Mathematics of Computation*, 73(247): 1582, July 2004. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/home.html; http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/S0025-5718-04-01695-3.dvi; http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/S0025-5718-04-01695-3.pdf; http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/S0025-5718-04-01695-3.ps; http://www.ams.org/mcom/2004-73-247/S0025-5718-04-01695-3/S0025-5718-04-01695-3.tex.

Shparlinski:2004:UDD

[Shp04b] Igor E. Shparlinski. On the uniformity of distribution of the decryption exponent in fixed encryption exponent RSA. *Information Processing Letters*, 92(3):143–147, November 15, 2004. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shparlinski:2005:PHS

[Shp05] Igor E. Shparlinski. Playing "hide-and-seek" with numbers: the hidden number problem, lattices, and exponential sums. In Garrett and Lieman [GL05], pages 153–177. ISBN 0-8218-3365-0. LCCN QA76.9.A25 P82 2005. URL `http://www.loc.gov/catdir/toc/fy0612/2005048178.html`.

Sun:2005:SSP

[SHT05] Hung-Min Sun, Bin-Tsan Hsieh, and Shin-Mu Tseng. On the security of some proxy blind signature schemes. *The Journal of Systems and Software*, 74(3):297–302, February 1, 2005. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Shumba:2006:THL

[Shu06] Rose Shumba. Teaching hands-on Linux host computer security. *ACM Journal on Educational Resources in Computing (JERIC)*, 6(3):5:1–5:??, September 2006. CODEN ???? ISSN 1531-4278.

Shyamasundar:2002:ACP

[Shy02] R. K. Shyamasundar. Analyzing cryptographic protocols in a reactive framework. *Lecture Notes in Computer Science*, 2294: 46–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2294/22940046.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2294/22940046.pdf`.

Silverman:2001:CLI

[Sil01] Joseph H. Silverman, editor. *Cryptography and lattices: International Conference, CaLC 2001, Providence RI, USA, March 29–30, 2001: Revised Papers*, volume 2146 of *Lecture Notes in Computer Science and Lecture Notes in Artificial Intelligence*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-42488-1 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C35 2001; QA267.A1 L43 no.2146. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2146.htm`; `http://www.springerlink.com/`

openurl.asp?genre=issue&issn=0302-9743&volume=2146.

Silverman:2005:ECC

[Sil05] Joseph H. Silverman. Elliptic curves and cryptography. In Garrett and Lieman [GL05], pages 91–112. ISBN 0-8218-3365-0. LCCN QA76.9.A25 P82 2005. URL http://www.loc.gov/catdir/toc/fy0612/2005048178.html.

Simon:2002:CRE

[Sim02] Denis Simon. Computing the rank of elliptic curves over number fields. *LMS Journal of Computation and Mathematics*, 5:7–17, 2002. CODEN ???? ISSN 1461-1570. URL http://www.lms.ac.uk/jcm/5/lms2000-006/.

Singh:1999:CBE

[Sin99] Simon Singh. *The code book: the evolution of secrecy from Mary, Queen of Scots, to quantum cryptography*. Doubleday, New York, NY, USA, 1999. ISBN 0-385-49531-5. xiii + 402 pp. LCCN Z103 .S56 1999. US$24.95. See also [AAG+00].

Singh:2000:CBE

[Sin00] Simon Singh. *The code book: the evolution of secrecy from Ancient Egypt to quantum cryptography*. Anchor Press/Doubleday, Garden City, NY, USA, 2000. ISBN 0-385-49532-3. xvii + 411 pp. LCCN Z103 .S56 1999. US$15.00. See also [AAG+00].

Singh:2001:DPK

[Sin01a] A. K. Singh. Deployment of public-key infrastructure in wireless data networks. *Lecture Notes in Computer Science*, 2094: 217–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2094/20940217.htm; http://link.springer-ny.com/link/service/series/0558/papers/2094/20940217.pdf.

Singh:2001:SSS

[Sin01b] Simon Singh. *The Science of Secrecy: The Secret History of Codes and Codebreaking*. Fourth Estate, London, UK, 2001. ISBN 1-84115-435-0. xi + 224 pp. LCCN Z103 .S57 2000. UK£14.99.

Singh:2002:CBH

[Sin02] Simon Singh. *The Code Book: How to Make It, Break It, Hack It, or Crack It*. Delacorte Press, New York, NY, USA, 2002. ISBN 0-385-72913-8. 263 (est.) pp. LCCN TK5102.92 .S56 2002.

Sinkov:2009:ECM

[Sin09] Abraham Sinkov. *Elementary cryptanalysis: a mathematical view*, volume 22 of *Anneli lax new mathematical library*. Mathematical Association of America, Washington, DC, USA, second edition, 2009. ISBN 0-88385-647-6. xiv + 212 pp. LCCN ???? URL `http://www.loc.gov/catdir/enhancements/fy0914/2009927623-d.html`; `http://www.loc.gov/catdir/enhancements/fy0914/2009927623-t.html`. Revised and updated by Todd Feil.

Stubblefield:2004:KRA

[SIR04] Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). *ACM Transactions on Information and System Security*, 7(2):319–332, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Sivonen:2006:MPF

[Siv06] Timo Sivonen. Measuring performance of FreeBSD disk encryption. *;login: the USENIX Association newsletter*, 31(5):40–45, October 2006. CODEN LOGNEM. ISSN 1044-6397. URL `https://www.usenix.org/publications/login/october-2006-volume-31-number-5/measuring-performance-freebsd-disk-encryption`.

Six:2005:HGS

[Six05] J. M. Six. Hidden gems [science and technology museums]. *IEEE Spectrum*, 42(1):70–71, January 2005. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Schnorr:2000:SSE

[SJ00] Claus Peter Schnorr and Markus Jakobsson. Security of signed ElGamal encryption. In *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, volume 1976 of *Lecture Notes in Comput. Sci.*, pages 73–89. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760073.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1976/19760073.pdf`.

Sucurovic:2005:JCX

[SJ05] S. Sucurovic and Z. Jovanovic. Java cryptography & X.509 authentication. *Dr. Dobb's Journal of Software Tools*, 30(2):40–42, 2005. CODEN DDJOEB. ISSN 1044-789X.

Schaumont:2009:GEI

[SJT09] Patrick R. Schaumont, Alex K. Jones, and Steve Trimberger. Guest Editors' introduction to security in reconfigurable systems design. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 2(1):1:1–1:??, March 2009. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Song:2000:TPA

[SK00] Boyeon Song and Kwangjo Kim. Two-pass authenticated key agreement protocol with key confirmation. *Lecture Notes in Computer Science*, 1977: 237–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1977/19770237.htm; http://link.springer-ny.com/link/service/series/0558/papers/1977/19770237.pdf`.

Seki:2001:DCR

[SK01a] Haruki Seki and Toshinobu Kaneko. Differential cryptanalysis of reduced rounds of GOST. *Lecture Notes in Computer Science*, 2012: 315–323, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stojanovski:2001:CBRa

[SK01b] T. Stojanovski and L. Kocarev. Chaos-based random number generators-part I: analysis [cryptography]. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Application*, 48(3):281–288, March 2001. CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic).

Sklavos:2003:DDR

[SK03] N. Sklavos and O. Koufopavlou. Data dependent rotations, a trustworthy approach for future encryption systems/ciphers: low cost and high performance. *Computers & Security*, 22(7):585–588, October 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404803007065`.

Sklavos:2005:ISH

[SK05a] N. Sklavos and O. Koufopavlou. Implementation of the SHA-2 hash family standard using FPGAs. *The Journal of Supercomputing*, 31(3): 227–248, March 2005. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=31&issue=3&spage=227`.

Stavrou:2005:CAS

[SK05b] Angelos Stavrou and Angelos D. Keromytis. Countering DoS attacks with stateless multipath overlays. In Meadows and Syverson [MS05b], pages 249–259. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Stabell-Kulo:2006:ESC

[SK06] Tage Stabell-Kulø. From the Editor: Security community — blurring the line between authentication and identification. *IEEE Distributed Systems Online*, 7 (2):1–5, February 2006. CODEN ???? ISSN 1541-4922 (print), 1558-1683 (electronic). URL http://csdl.computer.org/comp/mags/ds/2006/02/o2002.pdf.

Saldamli:2007:SME

[SK07] Gokay Saldamli and Cetin K. Koc. Spectral modular exponentiation. In Kornerup and Muller [KM07], pages 123–132. ISBN 0-7695-2854-6. ISSN 1063-6889. LCCN ???? URL http://www.lirmm.fr/arith18/.

Shu:2009:RCA

[SKG09] Chang Shu, Soonhak Kwon, and K. Gaj. Reconfigurable computing approach for Tate pairing cryptosystems over binary fields. *IEEE Transactions on Computers*, 58(9):1221–1237, September 2009. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4815221.

Sugita:2001:SRV

[SKI01] Makoto Sugita, Kazukuni Kobara, and Hideki Imai. Security of reduced version of the block cipher Camellia against truncated and impossible differential cryptanalysis. *Lecture Notes in Computer Science*, 2248: 193–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480193.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480193.pdf.

Sano:2000:PEA

[SKKS00] Fumihiko Sano, Masanobu Koike, Shinichi Kawamura, and Masue Shiba. Performance evaluation of AES finalists on the high-end Smart Card. In NIST [NIS00], pages 82–93. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/

encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Skolnikoff:2003:SS

[Sko03] Eugene B. Skolnikoff. Security and sanity. *IEEE Spectrum*, 40(4):13–14, April 2003. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Schindler:2001:IDC

[SKQ01] Werner Schindler, François Koeune, and Jean-Jacques Quisquater. Improving divide and conquer attacks against cryptosystems by better error detection/correction strategies. *Lecture Notes in Computer Science*, 2260: 245–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600245.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600245.pdf.

Srinathan:2002:ASC

[SKR02] K. Srinathan, M. V. N. Ashwin Kumar, and C. Pandu Rangan. Asynchronous secure communication tolerating mixed adversaries. *Lecture Notes in Computer Science*, 2501:224–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010224.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010224.pdf.

Sugita:2000:RAD

[SKU+00] Makoto Sugita, Kazukuni Kobara, Kazuhiro Uehara, Shuji Kubota, and Hideki Imai. Relationships among differential, truncated differential, impossible differential cryptanalyses against word-oriented block ciphers like RIJNDAEL, E2. In NIST [NIS00], pages 242–256. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.

pdf.

Schneier:2000:CTA

[SKW+00] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, and Niels Ferguson. Comments on Twofish as an AES candidate. In NIST [NIS00], pages 355–356. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Scharwaechter:2007:AAE

[SKW+07] Hanno Scharwaechter, David Kammler, Andreas Wieferink, Manuel Hohenauer, Kingshuk Karuri, Jianjiang Ceng, Rainer Leupers, Gerd Ascheid, and Heinrich Meyr. ASIP architecture exploration for efficient IPSec encryption: a case study. *ACM Transactions on Embedded Computing Systems*, 6(2):12:1–12:??, May 2007. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Sterbenz:2000:PAC

[SL00] Andreas Sterbenz and Peter Lipp. Performance of the AES candidate algorithms in Java. In NIST [NIS00], pages 161–168. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Shim:2005:SFA

[SL05a] Kyungah Shim and Young-Ran Lee. Security flaws in authentication and key establishment protocols for mobile communications. *Applied Mathematics and Computation*, 169(1):62–74, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Srivatsa:2005:SPS

[SL05b] Mudhakar Srivatsa and Ling Liu. Securing publish-subscribe overlay services with EventGuard. In Meadows and Syverson [MS05b], pages 289–298. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Skoudis:2006:CHR

[SL06] Ed Skoudis and Tom Liston. *Counter hack reloaded: a step-by-step guide to computer attacks and effective defenses*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, second edition, 2006. ISBN 0-13-148104-5 (paperback). ???? pp. LCCN TK5105.59 .S57 2006. URL http://www.loc.gov/catdir/toc/ecip0519/2005027164.html.

Stamp:2007:ACB

[SL07] Mark Stamp and Richard M. Low. *Applied cryptanalysis: breaking ciphers in the real world*. Wiley-Interscience, New York, NY, USA, 2007. ISBN 0-470-11486-X. xix + 401 pp. LCCN QA76.9.A25 S687 2007.

Sun:2009:CPR

[SL09] Fuyan Sun and Shutang Liu. Cryptographic pseudo-random sequence from the spatial chaotic map. *Chaos, solitons & fractals*, 41(5): 2216–2219, ???? 2009. CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic).

Su:2005:KPK

[SLC05] Pin-Chang Su, Erl-Huei Lu, and Henry Ker-Chang Chang. A knapsack public-key cryptosystem based on elliptic curve discrete logarithm. *Applied Mathematics and Computation*, 168(1): 40–46, September 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Shi:2005:HEC

[SLG+05] Weidong Shi, Hsien-Hsin S. Lee, Mrinmoy Ghosh, Chenghuai Lu, and Alexandra Boldyreva. High efficiency counter mode security architecture via prediction and precomputation. *ACM SIGARCH Computer Architecture News*, 33(2):14–24, May 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Shen:2003:SET

[SLH03] Jau-Ji Shen, Chih-Wei Lin, and Min-Shiang Hwang. Security enhancement for the timestamp-based password authentication scheme using smart cards. *Computers & Security*, 22(7):591–595, October 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803007090.

Sung:2000:PSS

[SLL+00] Jaechul Sung, Sangjin Lee, Jongin Lim, Seokhie Hong, and Sangjoon Park. Provable security for the Skipjack-like structure against differential cryptanalysis and linear cryptanalysis. *Lecture Notes in Computer Science*, 1976:274–288, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Salido:2007:EBE

[SLP07] Javier Salido, Loukas Lazos, and Radha Poovendran. Energy and bandwidth-efficient key distribution in wireless ad hoc networks: a cross-layer approach. *IEEE/ACM Transactions on Networking*, 15(6):1527–1540, December 2007. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Song:2001:DWF

[SLT01] Y. J. Song, R. Z. Liu, and T. N. Tan. Digital watermarking for forgery detection in printed materials. *Lecture Notes in Computer Science*, 2195: 403–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950403.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2195/21950403.pdf`.

Solar-Lezama:2006:CSF

[SLTB+06] Armando Solar-Lezama, Liviu Tancau, Rastislav Bodik, Sanjit Seshia, and Vijay Saraswat. Combinatorial sketching for finite programs. *ACM SIGPLAN Notices*, 41(11):404–415, November 2006. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Sarkar:2000:CNB

[SM00a] Palash Sarkar and Subhamoy Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. *Lecture Notes in Computer Science*, 1807:485–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070485.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1807/18070485.pdf`.

Sarkar:2000:NBC

[SM00b] Palash Sarkar and Subhamoy Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In Bellare [Bel00], pages 515–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800515.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800515.pdf.

Sebag-Montefiore:2000:EBC

[SM00c] Hugh Sebag-Montefiore. *Enigma: the battle for the code*. John Wiley and Sons, Inc., New York, NY, USA, 2000. ISBN 0-471-40738-0 (cloth). x + 422 pp. LCCN D810.C88 S43 2000. URL http://www.loc.gov/catdir/bios/wiley043/00043920.html; http://www.loc.gov/catdir/description/wiley035/00043920.html; http://www.loc.gov/catdir/toc/onix06/00043920.html.

Sarkar:2001:EIL

[SM01] P. Sarkar and S. Maitra. Efficient implementation of "large" stream cipher systems. *Lecture Notes in Computer Science*, 2162: 319–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620319.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620319.pdf.

Satoh:2002:SHS

[SM02] Akashi Satoh and Sumio Morioka. Small and high-speed hardware architectures for the 3GPP standard cipher KASUMI. *Lecture Notes in Computer Science*, 2433:48–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330048.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330048.pdf.

Sarkar:2003:EIC

[SM03a] P. Sarkar and S. Maitra. Efficient implementation of cryptographically useful "large" Boolean functions. *IEEE Transactions on Computers*, 52(4):410–417, April 2003. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1190582.

Satoh:2003:UHA

[SM03b] Akashi Satoh and Sumio Morioka. Unified hardware architecture for 128-bit block ciphers AES and Camellia. In Walter et al. [WKP03], pages 304–318. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240`.

Sebag-Montefiore:2005:EBC

[SM05] Hugh Sebag-Montefiore. *Enigma: the battle for the code*. John Wiley and Sons, Inc., New York, NY, USA, 2005. ISBN 0-471-49035-0. 352 + 16 pp. LCCN ????

Sebag-Montefiore:2007:EBC

[SM07a] Hugh Sebag-Montefiore. *Enigma: the battle for the code*. Barnes and Noble, New York, NY, USA, 2007. ISBN 0-7607-9118-X. x + 422 + 16 pp. LCCN D810.C88 S43 2007.

Simos:2007:CMS

[SM07b] Theodore E. Simos and George Maroulis, editors. *Computation in Modern Science and Engineering: Proceedings of the [Fifth] International Conference on Computational Methods in Science and Engineering 2007 (ICCMSE 2007), Corfu, Greece, 25–30 September 2007*, volume 2A, 2B of *AIP Conference Proceedings (#963)*. American Institute of Physics, Woodbury, NY, USA, 2007. ISBN 0-7354-0476-3 (set), 0-7354-0477-1 (vol. 1), 0-7354-0478-X (vol. 2). ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. LCCN Q183.9 .I524 2007. URL `http://www.springer.com/physics/atoms/book/978-0-7354-0478-6`.

Smith-Miles:2008:CDP

[SM08] Kate A. Smith-Miles. Cross-disciplinary perspectives on meta-learning for algorithm selection. *ACM Computing Surveys*, 41(1):6:1–6:25, December 2008. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Seyedzadeh:2011:IES

[SM11] S. M. Seyedzadeh and S. Mirzakuchaki. Image encryption scheme based on Choquet fuzzy integral with pseudo-random keystream generator. In *2011 International Symposium on Artificial Intelligence and Signal Processing (AISP)*, pages 101–106. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.`

org/stamp/stamp.jsp?tp=&arnumber=5960982.

Smart:2001:CDF

[Sma01] N. P. Smart. A comparison of different finite fields for elliptic curve cryptosystems. *Computers and Mathematics with Applications*, 42(1-2):91–100, 2001. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Smart:2003:ACU

[Sma03a] Nigel P. Smart. Access control using pairing based cryptography. In Joye [Joy03b], pages 111–121. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Smart:2003:AGR

[Sma03b] Nigel P. Smart. An analysis of Goubin's refined power analysis attack. In Walter et al. [WKP03], pages 281–290. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Smart:2005:CCI

[Sma05] Nigel P. Smart, editor. *Cryptography and Coding: 10th IMA international Conference, Cirencester, UK, December 19–21, 2005. Proceedings*, volume 3796 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-30276-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3796.

Small:2006:USR

[Sma06] Mike Small. Unify and simplify: re-thinking identity management. *Network Security*, 2006(7):11–14, July 2006. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485806704111.

Smith:2000:ABS

[Smi00] Tim Smith. Authentication by biometric smart card. *Network Security*, 2000(6): 5, June 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485800060116`.

Smith:2001:IK

[Smi01a] David Smith. Implementing Kerberos. *Sys Admin: The Journal for UNIX Systems Administrators*, 10 (12):28, 30, 32, 34–38, December 2001. CODEN SYADE7. ISSN 1061-2688.

Smith:2001:ECB

[Smi01b] Michael Smith. *The Emperor's Codes: Bletchley Park and the breaking of Japan's secret ciphers*. Bantam Doubleday Dell Publishing Group Inc., 666 Fifth Avenue, New York, NY 10130, USA, 2001. ISBN 0-553-81320-X (paperback). 410 + 14 pp. LCCN ???? UK£7.99.

Smith:2001:APP

[Smi01c] Richard E. Smith. *Authentication: From Passwords to Public Keys*. Addison-Wesley, Reading, MA, USA, 2001. ISBN 0-201-61599-1. 549 pp. LCCN QA76.9.A25 S65 2002. US$44.99.

Smith:2002:OAP

[Smi02] Sean W. Smith. Outbound authentication for programmable secure coprocessors. *Lecture Notes in Computer Science*, 2502: 72–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2502/25020072.htm`; `http://link.springer.de/link/service/series/0558/papers/2502/25020072.pdf`.

Smith:2003:FTT

[Smi03] B. Smith. Fort TV [TV show e-mail transmission prevention]. *IEEE Spectrum*, 40 (5):30–32, May 2003. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Smith:2008:CFI

[Smi08] Don Smith. The challenge of federated identity management. *Network Security*, 2008(4):7–9, April 2008. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485808700515`.

Smolin:2004:EDE

[Smo04] J. A. Smolin. The early days of experimental quantum cryptography. *IBM*

Journal of Research and Development, 48(1):47–??, ???? 2004. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http://www.research.ibm.com/journal/rd/481/smolin.pdf`.

Seamons:2009:IPS

[SMP+09] Kent Seamons, Neal McBurnett, Tim Polk, et al., editors. *IDtrust2009: proceedings of the 8th Symposium on Identity and Trust on the Internet: April 14–16, 2009, Gaitherburg, Maryland, USA*. ACM Press, New York, NY 10036, USA, 2009. ISBN 1-60558-474-6. LCCN QA76.9.A25 S954 2009. URL `http://portal.acm.org/toc.cfm?id=1527017&coll=portal&dl=ACM`.

Satoh:2001:CRH

[SMTM01] Akashi Satoh, Sumio Morioka, Kohji Takano, and Seiji Munetoh. A compact Rijndael hardware architecture with S-box optimization. *Lecture Notes in Computer Science*, 2248: 239–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480239.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2248/22480239.pdf`.

Strembeck:2004:IAE

[SN04] Mark Strembeck and Gustaf Neumann. An integrated approach to engineer and enforce context constraints in RBAC environments. *ACM Transactions on Information and System Security*, 7(3):392–427, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Schlager:2007:EAA

[SN07] Christian Schläger and Thomas Nowey. On the effects of authentication and authorisation infrastructures on e-commerce activities. *International Journal of Computer Systems Science and Engineering*, 22(5):??, September 2007. CODEN CSSEEI. ISSN 0267-6192.

Sakai:2000:NDS

[SNI00] Hideaki Sakai, Noriko Nakamura, and Yoshihide Igarashi. A new definition of semantic security for public-key encryption schemes. *Sūrikaisekikenkyūsho Kōkyūroku*, 1148:112–117, 2000. Theoretical foundations of computer science: toward a paradigm for computing in the 21st century (Japanese) (Kyoto, 2000).

Srinathan:2004:OPS

[SNR04] K. Srinathan, Arvind Narayanan, and C. Pandu Rangan. Optimal perfectly secure message transmission. In Franklin [Fra04], pages 545–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Safavi-Naini:2000:STT

[SNW00] Reihaneh Safavi-Naini and Yejing Wang. Sequential traitor tracing. In Bellare [Bel00], pages 316–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800316.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800316.pdf.

Safavi-Naini:2001:BAG

[SNW01] Rei Safavi-Naini and Huaxiong Wang. Broadcast authentication for group communication. *Theoretical Computer Science*, 269 (1–2):1–21, October 28, 2001. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.nl/gej-ng/10/41/16/219/27/27/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/219/27/27/article.pdf.

Safavi-Naini:2001:LAC

[SNWX01] R. Safavi-Naini, H. Wang, and C. Xing. Linear authentication codes: Bounds and constructions. *Lecture Notes in Computer Science*, 2247:127–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470127.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470127.pdf.

Sanchez:2001:RNM

[SOHS01] David Sánchez, Agustín Orfila, Julio César Hernández, and José María Sierra. Robust new method in frequency domain watermarking. *Lecture Notes in Computer Science*, 2200: 166–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/

bibs/2200/22000166.htm; http://link.springer-ny.com/link/service/series/0558/papers/2200/22000166.pdf.

Slind:2007:PPS

[SOIG07] Konrad Slind, Scott Owens, Juliano Iyoda, and Mike Gordon. Proof producing synthesis of arithmetic and cryptographic hardware. *Formal Aspects of Computing*, 19(3):343–362, August 2007. CODEN FACME5. ISSN 0934-5043 (print), 1433-299X (electronic). URL http://link.springer.com/article/10.1007/s00165-007-0028-5.

Song:2000:ISC

[Son00] JooSeok Song, editor. *Information security and cryptology — ICISC'99: second international conference, Seoul, Korea, December 9–10, 1999: proceedings*, volume 1787 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-67380-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1787.

Shigetomi:2002:ALS

[SOOI02] Rie Shigetomi, Akira Otsuka, Takahide Ogawa, and Hideki Imai. An anonymous loan system based on group signature scheme. *Lecture Notes in Computer Science*, 2433:244–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330244.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330244.pdf.

Satoh:2000:HSM

[SOTD00] Akashi Satoh, Nobuyuki Ooba, Kohji Takano, and Edward D'Avignon. High-speed MARS hardware. In NIST [NIS00], pages 305–316. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Smith:1979:UFM

[SP79] Donald R. Smith and James T. Palmer. Universal fixed messages and the

Rivest–Shamir–Adleman cryptosystem. *Mathematika*, 26 (1):44–52, 1979. CODEN MTKAAB. ISSN 0025-5793.

Shelfer:2002:SCE

[SP02] Katherine M. Shelfer and J. Drew Procaccino. Smart card evolution. *Communications of the Association for Computing Machinery*, 45(7):83–88, July 2002. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Sumii:2003:LRE

[SP03] Eijiro Sumii and Benjamin C. Pierce. Logical relations for encryption. *Journal of Computer Security*, 11(4):521–554, ???? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Solachidis:2004:WPL

[SP04] Vassilios Solachidis and Ioannis Pitas. Watermarking polygonal lines using Fourier descriptors. *IEEE Computer Graphics and Applications*, 24(3):44–51, May/June 2004. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic). URL `http://csdl.computer.org/comp/mags/cg/2004/03/g3044abs.htm; http://csdl.computer.org/dl/mags/cg/2004/03/g3044.htm; http://csdl.computer.org/dl/mags/cg/2004/03/g3044.pdf`.

Schielzeth:2005:RQN

[SP05] Daniel Schielzeth and Michael E. Pohst. On real quadratic number fields suitable for cryptography. *Experimental Mathematics*, 14(2):189–197, ???? 2005. CODEN ???? ISSN 1058-6458 (print), 1944-950X (electronic). URL `http://projecteuclid.org/euclid.em/1128100131`.

Shahruz:2002:DNC

[SPG02] S. M. Shahruz, A. K. Pradeep, and R. Gurumoorthy. Design of a novel cryptosystem based on chaotic oscillators and feedback inversion. *Journal of Sound and Vibration*, 250 (4):762–771, 2002. CODEN JSVIAG. ISSN 0022-460X.

Standaert:2006:SSE

[SPGQ06] François-Xavier Standaert, Gilles Piret, Neil Gershenfeld, and Jean-Jacques Quisquater. SEA: A scalable encryption algorithm for small embedded applications. *Lecture Notes in Computer Science*, 3928: 222–236, 2006. CODEN LNCSD9. ISBN 3-540-33311-8 (print), 3-540-33312-6 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/11733447_16`.

Singaravelu:2006:RTC

[SPHH06] Lenin Singaravelu, Calton Pu, Hermann Härtig, and Christian Helmuth. Reducing TCB complexity for security-sensitive applications: three case studies. *Operating Systems Review*, 40(4):161–174, October 2006. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Sun:2008:BWN

[SPK08] Shusen Sun, Zhigeng Pan, and Tae-Wan Kim. Blind watermarking of non-uniform B-spline surfaces. *International Journal of Image and Graphics (IJIG)*, 8(3):439–454, July 2008. CODEN ???? ISSN 0219-4678.

Stern:2002:FAP

[SPMLS02] Jacques Stern, David Pointcheval, John Malone-Lee, and Nigel P. Smart. Flaws in applying proof methodologies to signature schemes. In Yung [Yun02a], pages 93–110. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420093.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420093.pdf.

Springer:2003:BRB

[Spr03] William M. Springer II. Book review: *Cryptography: Theory and Practice*, second edition by Douglas R. Stinson. CRC Press. *ACM SIGACT News*, 34 (4):22–25, December 2003. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Sti95, Sti02, Sti06c].

Song:2001:ANL

[SQ01] Zhimin Song and Sihan Qing. Applying NCP logic to the analysis of SSL 3.0. *Lecture Notes in Computer Science*, 2229: 155–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290155.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290155.pdf.

Shin:2000:ANT

[SR00] Sang Uk Shin and Kyung Hyune Rhee. All-or-nothing transform and remotely keyed encryption protocols. In *Public key cryptography (Melbourne, 2000)*, volume 1751 of *Lecture Notes in Comput. Sci.*, pages 178–195. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000.

Sanchez-Reillo:2001:IBA

[SR01] Raul Sanchez-Reillo. Including biometric authentication in a smart card operating system. *Lecture Notes in Computer Science*, 2091:342–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2091/20910342.htm; http://link.springer-ny.com/link/service/series/0558/papers/2091/20910342.pdf.

StDenis:2006:BMI

[SR06] Tom St Denis and Greg Rose. *BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic*. Syngress Publishing, Inc., Rockland, MA, USA, 2006. ISBN 1-59749-112-8. xviii + 296 pp. LCCN QA402.5 .S73 2006. US$49.95. URL http://www.oreilly.com/catalog/1597491128/index.html.

Stipcevic:2007:QRN

[SR07] M. Stipçević and B. Medved Rogina. Quantum random number generator. *Review of Scientific Instruments*, 78 (045104):9, 2007. CODEN RSINAK. ISSN 1089-7623, 0034-6748. URL http://qrbg.irb.hr/0609043v2.pdf. arXiv:quant-ph/0609043v2.

Samarati:2001:AMP

[SRJ01] Pierangela Samarati, Michael K. Reiter, and Sushil Jajodia. An authorization model for a public key management service. *ACM Transactions on Information and System Security*, 4(4):453–482, November 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Standaert:2003:EIR

[SRQL03] François-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat. Efficient implementation of Rijndael encryption in reconfigurable hardware: Improvements and design tradeoffs. In Walter et al. [WKP03], pages 334–350. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Sarkar:2001:PAE

[SS01a] P. Sarkar and P. J. Schellenberg. A parallel algorithm for extending cryptographic hash functions. *Lecture Notes in Computer Science*, 2247:40–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470040.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470040.pdf`.

Stubblebine:2001:AAF

[SS01b] Stuart G. Stubblebine and Paul F. Syverson. Authentic attributes with fine-grained anonymity protection. *Lecture Notes in Computer Science*, 1962: 276–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620276.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620276.pdf`.

Seznec:2003:HUL

[SS03] André Seznec and Nicolas Sendrier. HAVEGE: a user-level software heuristic for generating empirically strong random numbers. *ACM Transactions on Modeling and Computer Simulation*, 13(4):334–346, October 2003. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Swiderski:2004:TM

[SS04] Frank Swiderski and Window Snyder. *Threat modeling*. Microsoft Press, Redmond, WA, USA, 2004. ISBN 0-7356-1991-3 (paperback). xv + 259 pp. LCCN QA76.9.A25 S934 2004.

Seddik:2009:IWB

[SSFC09] Hassen Seddik, Mounir Sayadi, Farhat Fnaiech, and Mohamed Cheriet. Image watermarking based on the Hessenberg transform. *International Journal of Image and Graphics (IJIG)*, 9 (3):411–433, July 2009. CODEN ???? ISSN 0219-4678.

Shi:2008:UAU

[SSM+08] Minghui Shi, Xuemin (Sherman) Shen, Jon W. Mark, Dongmei Zhao, and Yixin Jiang. User authentication and undeniable billing support for agent-based roaming service in WLAN/cellular integrated mobile networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 52(9):1693–1702, June 26, 2008. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Susilo:2000:NEF

[SSNGS00] Willy Susilo, Rei Safavi-Naini, Marc Gysin, and Jennifer Seberry. A new and efficient fail-stop signature scheme. *The Computer Journal*, 43(5):430–437, ???? 2000. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_43/Issue_05/430430.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_43/Issue_05/pdf/430430.pdf.

Scambray:2006:HEW

[SSS06] Joel Scambray, Mike Shema, and Caleb Sima. *Hacking exposed: Web applications*. McGraw-Hill, New York, NY, USA, second edition, 2006. ISBN 0-07-226299-0 (paperback). xxix + 520 pp. LCCN TK5105.59 .S32 2006.

Schmidt-Samoa:2006:AFW

[SSST06] K. Schmidt-Samoa, O. Semay, and T. Takagi. Analysis of fractional window recoding methods and their application to elliptic curve cryptosystems. *IEEE Transactions on Computers*, 55(1):48–57, January 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1545750.

StPierre:2000:TFA

[St.00] Jim St. Pierre. Two-factor authentication added to PKI solutions. *Network Security*, 2000(5):6, May 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800050182.

Sakurai:2001:NSS

[ST01a] Kouichi Sakurai and Tsuyoshi Takagi. New semantically secure public-key cryptosystems from the RSA-primitive. *Lecture Notes in Computer Science*, 2274:1–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2274/22740001.htm; http://link.springer-ny.com/link/service/series/0558/papers/2274/22740001.pdf.

Shamir:2001:IOO

[ST01b] Adi Shamir and Yael Tauman. Improved online/offline signature schemes. In Kilian [Kil01a], pages 355–?? ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25 C79 2001; QA267.A1 L43 no.2139.

UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390355.htm; http://link.springer-ny.com/link/service/series/0558/papers/2139/21390355.pdf.

Stern:2001:ADW

[ST01c] Julien P. Stern and Jean-Pierre Tillich. Automatic detection of a watermarked document using a private key. *Lecture Notes in Computer Science*, 2137: 258–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370258.htm; http://link.springer-ny.com/link/service/series/0558/papers/2137/21370258.pdf.

Stinson:2001:SAC

[ST01d] Douglas R. Stinson and Stafford Tavares, editors. *Selected areas in cryptography: 7th annual international workshop, SAC 2000, Waterloo, Ontario, Canada, August 14–15, 2000: proceedings*, volume 2012 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-42069-X (paperback). LCCN QA76.9.A25 S22 2000; QA267.A1 L43 no.2012. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2012.htm.

Sakurai:2002:SMP

[ST02] Kouichi Sakurai and Tsuyoshi Takagi. On the security of a modified Paillier public-key primitive. *Lecture Notes in Computer Science*, 2384:436–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840436.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840436.pdf.

Satoh:2003:SDF

[ST03a] A. Satoh and K. Takano. A scalable dual-field elliptic curve cryptographic processor. *IEEE Transactions on Computers*, 52 (4):449–460, April 2003. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1190586.

Shamir:2003:FLN

[ST03b] Adi Shamir and Eran Tromer. Factoring large numbers with the TWIRL device. In Boneh [Bon03], pages 1–26. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Spivak:2006:SPT

[ST06] Michal Spivak and Sivan Toledo. Storing a persistent transactional object heap on flash memory. *ACM SIGPLAN Notices*, 41(7):22–33, July 2006. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Stallings:2000:SSC

[Sta00] William Stallings. The SET Standard and E-commerce. *Dr. Dobb's Journal of Software Tools*, 25(11):30, 32, 34, 36, November 2000. CODEN DDJOEB. ISSN 1044-789X.

Stallings:2002:CNS

[Sta02a] William Stallings. *Cryptography and network security: principles and practice*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, third edition, 2002. ISBN 0-13-091429-0. 696 (est.) pp.

Standboge:2002:ENO

[Sta02b] James Standboge. Encrypted NFS with OpenSSH and Linux. *Sys Admin: The Journal for UNIX Systems Administrators*, 11(3):30, 32–34, March 2002. CODEN SYADE7. ISSN 1061-2688.

Stajano:2003:SCU

[Sta03] Frank Stajano. The security challenges of ubiquitous computing. In Walter et al. [WKP03], page 1. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Stanik:2005:NLO

[Sta05] John Stanik. News 2.0: Losing our edge? the real cost of Linux; say no to crackberries. *ACM Queue: Tomorrow's Computing Today*, 3(5):14, June 2005. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Stamp:2006:ISP

[Sta06] Mark Stamp. *Information security: principles and practice*. Wiley-Interscience, New York, NY, USA, 2006. ISBN 0-471-73848-4 (cloth). xxi + 390 pp. LCCN QA76.9.A25 S69 2006. URL http://www.loc.gov/catdir/enhancements/fy0645/2005005152-b.html; http://www.loc.gov/catdir/enhancements/fy0645/2005005152-d.html; http://www.loc.gov/catdir/toc/ecip058/2005005152.html.

Sterlicchi:2000:SCD

[Ste00] John Sterlicchi. Software companies disappointed by encryption draft. *Network Security*, 2000(1):4, January 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800866477.

Steinwandt:2001:LTP

[Ste01] Rainer Steinwandt. Loopholes in two public key cryptosystems using the modular group. *Lecture Notes in Computer Science*, 1992: 180–189, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920180.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920180.pdf.

Stefanek:2002:ISB

[Ste02] George L. Stefanek. *Information security best practices: 205 basic rules*. Newnes Press, Amsterdam, The Netherlands and Boston, MA, USA, 2002. ISBN 1-878707-96-5. xii + 194 pp. LCCN QA76.9.A25S744 2002. US$29.95.

Steele:2005:PPT

[Ste05a] Corey Steele. Paranoid penguin: Two-factor authentication. *Linux Journal*, 2005 (139):10, November 2005. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Steil:2005:MMM

[Ste05b] Michael Steil. 17 mistakes Microsoft made in the Xbox security system. Report, Xbox Linux Project, December 2005. 13 pp. URL http://events.ccc.de/congress/2005/fahrplan/attachments/591-paper_xbox.pdf.

Stern:2005:MLF

[Ste05c] Richard H. Stern. Micro law: FTC cracks down on spyware and PC hijacking, but not true lies. *IEEE Micro*, 25 (1):6–7, 100–101, January/

February 2005. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL `http://csdl.computer.org/dl/mags/mi/2005/01/m1006.htm`; `http://csdl.computer.org/dl/mags/mi/2005/01/m1006.pdf`.

Stein:2008:ENT

[Ste08] William Stein. *Elementary number theory: primes, congruences, and secrets*, volume 666 of *Undergraduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 0-387-85524-6. 175 (est.) pp. LCCN ????

Stinson:1995:CTP

[Sti95] Douglas R. (Douglas Robert) Stinson. *Cryptography: theory and practice*. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1995. ISBN 0-8493-8521-0. 434 pp. LCCN QA268 .S75 1995.

Stinson:2001:C

[Sti01] Douglas R. Stinson. *Cryptography*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, second edition, 2001. ISBN 1-58488-206-9. 512 (est) pp. LCCN QA268 .S75 2002. UK£49.99.

Stinson:2002:CTP

[Sti02] Douglas R. (Douglas Robert) Stinson. *Cryptography: theory and practice*. The CRC Press series on discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, second edition, 2002. ISBN 1-58488-206-9. 339 pp. LCCN QA268 .S75 2002.

Stieber:2006:OH

[Sti06a] Anthony J. Stieber. OpenSSL hacks. *Linux Journal*, 2006 (147):??, July 2006. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Stieber:2006:GH

[Sti06b] Tony Stieber. GnuPG hacks. *Linux Journal*, 2006 (143):2, March 2006. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Stinson:2006:CTP

[Sti06c] Douglas R. (Douglas Robert) Stinson. *Cryptography: theory and practice*. The CRC Press series on discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, third edition, 2006. ISBN 1-58488-508-4 (hardcover). 593

pp. LCCN QA268 .S75 2006. URL http://www.loc.gov/catdir/enhancements/fy0647/2006272493-d.html.

Stipcevic:2011:QRN

[Sti11] M. Stipcevic. Quantum random number generators and their use in cryptography. In *2011 Proceedings of the 34th International Convention MIPRO*, pages 1474–1479. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5967293.

Shimoyama:2002:MLC

[STK02] Takeshi Shimoyama, Masahiko Takenaka, and Takeshi Koshiba. Multiple linear cryptanalysis of a reduced round RC6. *Lecture Notes in Computer Science*, 2365:76–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650076.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650076.pdf.

Stone:2001:CI

[Sto01] Jonathan Richard Stone. *Checksums and the Internet*. Ph.D. dissertation, Department of Computer Science, Stanford University, Stanford, CA, USA, 2001. 228 pp. URL http://wwwlib.umi.com/dissertations/fullcit/3028177.

Struif:2001:UBU

[Str01a] Bruno Struif. Use of biometrics for user verification in electronic signature smartcards. *Lecture Notes in Computer Science*, 2140:220–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400220.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400220.pdf.

Strunk:2001:JQJ

[Str01b] Elisabeth Strunk. Java Q&A: Java & NT authentication. *Dr. Dobb's Journal of Software Tools*, 26(2):145–146, 148, February 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ftp/2001/2001_02/jqa0201.txt.

Strubinger:2002:HBS

[Str02] Ray Strubinger. A home-grown backup solution utilizing RSA keys, SSH, and tar. *Sys Admin: The Journal for UNIX Systems Administrators*, 11(4):37–

38, April 2002. CODEN SYADE7. ISSN 1061-2688.

Stytz:2004:BRW

[Sty04] Martin R. Stytz. Book reviews: Wireless world order [*How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN* by Lee Barken]; no need to fear [*Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, by Bruce Schneier]. *IEEE Security & Privacy*, 2(1):20–21, January/February 2004. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://csdl.computer.org/comp/mags/sp/2004/01/j1020abs.htm`; `http://csdl.computer.org/dl/mags/sp/2004/01/j1020.pdf`.

Saxena:2007:TCP

[STY07] Nitesh Saxena, Gene Tsudik, and Jeong Hyun Yi. Threshold cryptography in P2P and MANETs: The case of access control. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(12):3632–3649, August 22, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Shaltiel:2007:LEU

[SU07] Ronen Shaltiel and Christopher Umans. Low-end uniform hardness vs. randomness tradeoffs for AM. In ACM [ACM07], pages 430–439. ISBN 1-59593-631-9. LCCN QA75.5 .A22 2007.

Sugihara:2001:PCD

[Sug01] Ryo Sugihara. Practical capacity of digital watermarks. *Lecture Notes in Computer Science*, 2137: 316–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370316.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2137/21370316.pdf`.

Sugita:2003:DRW

[Sug03] Hiroshi Sugita. Dynamic random Weyl sampling for drastic reduction of randomness in Monte Carlo integration. *Mathematics and Computers in Simulation*, 62(3–6):529–537, March 3, 2003. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475402002318`.

Sullivan:2005:CFI

[Sul05] Roger K. Sullivan. The case for federated identity. *Network Security*, 2005(9):15–19, September 2005. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348580570283X.

Sun:2000:DRR

[Sun00a] H.-M.-Min Sun. On the dealer's randomness required in perfect secret sharing schemes with access structures of constant rank. *International Journal of Foundations of Computer Science (IJFCS)*, 11 (2):263–282, 2000. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Sun:2000:ESM

[Sun00b] Hung-Min Sun. Enhancing the security of the McEliece public-key cryptosystem. *Journal of Information Science and Engineering*, 16 (6):799–812, 2000. CODEN JINEEY. ISSN 1016-2364.

Sun:2002:IIR

[Sun02] Hung-Min Sun. Improving the information rate of a private-key cryptosystem based on product codes. *Informatica (Vilnius)*, 13(1): 105–110, 2002. ISSN 0868-4952.

Sun:2005:UMS

[Sun05] Qibin Sun. Understanding multimedia security. *IEEE MultiMedia*, 12(4): 88–89, October/December 2005. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://csdl.computer.org/comp/mags/mu/2005/04/u4088.pdf.

Seidl:2008:FOV

[SV08a] Helmut Seidl and Kumar Neeraj Verma. Flat and one-variable clauses: Complexity of verifying cryptographic protocols with single blind copying. *ACM Transactions on Computational Logic*, 9(4):28:1–28:??, August 2008. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Shaltiel:2008:HAP

[SV08b] Ronen Shaltiel and Emanuele Viola. Hardness amplification proofs require majority. In ACM [ACM08], pages 589–598. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Sebe:2007:SMO

[SVDF07] Francesc Sebé, Alexandre Viejo, and Josep Domingo-Ferrer. Secure many-to-one symbol transmission for implementation on smart cards. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(9):2299–2307, June 20, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Shmueli:2009:DEO

[SVEG09] Erez Shmueli, Ronen Vaisenberg, Yuval Elovici, and Chanan Glezer. Database encryption: an overview of contemporary challenges and design considerations. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 38 (3):29–34, September 2009. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Smith:2000:CIR

[SVW00] Michael Smith, Paul Van Oorschot, and Michael Willett. Cryptographic information recovery using key recovery. *Computers & Security*, 19(1):21–27, January 1, 2000. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404800863580.

Schneier:2000:PCF

[SW00a] Bruce Schneier and Doug Whiting. A performance comparison of the five AES finalists. In NIST [NIS00], pages 123–135. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Sun:2000:AFA

[SW00b] Yongxing Sun and Xinmei Wang. An approach to finding the attacks on the cryptographic protocols. *Operating Systems Review*, 34(3): 19–28, July 2000. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Stubblebine:2002:ALF

[SW02] S. G. Stubblebine and R. N. Wright. An authentication logic with formal semantics supporting synchronization, revocation, and recency. *IEEE Transactions on Software Engineering*, 28(3): 256–285, March 2002. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=991320.

Shim:2005:WIB

[SW05a] Kyungah Shim and Sungsik Woo. Weakness in ID-based one round authenticated tripartite multiple-key agreement protocol with pairings. *Applied Mathematics and Computation*, 166 (3):523–530, July 26, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Stuck:2005:HVC

[SW05b] B. Stuck and M. Weingarten. How venture capital thwarts innovation. *IEEE Spectrum*, 42(4):50–55, April 2005. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Shieh:2006:ERM

[SW06] Wen-Gong Shieh and Jian-Min Wang. Efficient remote mutual authentication and key agreement. *Computers & Security*, 25(1):72–77, February 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404805001719.

Swaine:2001:PPSa

[Swa01] Michael Swaine. Programming paradigms: Secrets and lies. *Dr. Dobb's Journal of Software Tools*, 26(4): 125–127, April 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Swenson:2008:MCT

[Swe08] Christopher Swenson. *Modern cryptanalysis: techniques for advanced code breaking*. John Wiley and Sons, Inc., New York, NY, USA, 2008. ISBN 0-470-13593-X (cloth). xxviii + 236 pp. LCCN QA76.9.A25 S932 2008. URL http://www.loc.gov/catdir/enhancements/fy0806/2007051636-d.html; http://www.loc.gov/catdir/enhancements/fy0808/2007051636-t.html; http://www.loc.gov/catdir/enhancements/fy0810/2007051636-b.html.

Song:2005:ISG

[SWH05] Lin Song, Biao Wang, and Dequan He. An improved scheme for group signature. In Han et al. [HYZ05b], pages 96–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Sun:2009:TDS

[SWH+09] Hung-Min Sun, Mu-En Wu, M. Jason Hinek, Cheng-Ta Yang, and Vincent S. Tseng. Trading decryption for speeding encryption in Rebalanced-RSA. *The Journal of Systems and Software*, 82(9):1503–1512, September 2009. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Swire:2005:SMI

[Swi05] Peter P. Swire. Security market: incentives for disclosure of vulnerabilities. In Meadows and Syverson [MS05b], page 405. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Stevenson:2005:SCI

[SWR05] Daniel E. Stevenson, Michael R. Wick, and Steven J. Ratering. Steganography and cartography: interesting assignments that reinforce machine representation, bit manipulation, and discrete structures concepts. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 37(1):277–281, March 2005. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Song:2007:TAK

[SWT07] Dawn Xiaodong Song, David Wagner, and Xuqing Tian. Timing analysis of keystrokes and timing attacks on SSH. Report, University of California, Berkeley, Berkeley, CA, USA, July 15, 2007. URL `http://www.cs.berkeley.edu/~dawnsong/papers/ssh-timing.pdf`.

Shujun:2001:PRB

[SXY01] L. Shujun, M. Xuanqin, and C. Yuanlong. Pseudorandom bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. *Lecture Notes in Computer Science*, 2247: 316–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470316.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470316.pdf`.

Seo:2001:CDA

[SY01a] Jin S. Seo and Chang D. Yoo. Correlation detection of asymmetric watermark. *Lecture Notes in Computer Science*, 2195: 638–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950638.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950638.pdf`.

Shi:2001:NSF

[SY01b] Jiaoying Shi and Kaixiang Yi. New semi-fragile authentication watermarking. *Lecture Notes in Computer Science*, 2195: 969–??, 2001. CODEN LNCSD9. ISSN 0302-

9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950969.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950969.pdf.

Sun:2006:PBA

[SY06] Hung-Min Sun and Her-Tyan Yeh. Password-based authentication and key distribution protocols with perfect forward secrecy. *Journal of Computer and System Sciences*, 72(6):1002–1011, September 2006. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000006000481.

Syed:2000:CLA

[Sye00] Furqan Syed. Children of DES: a look at the Advanced Encryption Standard. *Network Security*, 2000(9):11–12, September 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800090267.

Sun:2005:CSS

[SYLC05] Qibin Sun, Shuiming Ye, Ching-Yung Lin, and Shih-Fu Chang. A crypto signature scheme for image authentication over wireless channel. *International Journal of Image and Graphics (IJIG)*, 5(1):135–??, January 2005. CODEN ???? ISSN 0219-4678.

Syverson:2002:FCI

[Syv02] Paul F. Syverson, editor. *Financial Cryptography: 5th International Conference, FC 2001, Grand Cayman, British West Indies, February 19–22, 2001. Proceedings*, volume 2339 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-44079-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 2001. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2339.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2339.

Shimoyama:2002:BCS

[SYY+02] Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima, Naoya Torii, and Hidema Tanaka. The block cipher SC2000. *Lecture Notes in Computer Science*, 2355:312–??, 2002. CODEN LNCSD9. ISSN 0302-

9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550312.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550312.pdf.

Steinfeld:2001:ALE

[SZ01] Ron Steinfeld and Yuliang Zheng. An advantage of low-exponent RSA with modulus primes sharing least significant bits. *Lecture Notes in Computer Science*, 2020:52–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200052.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200052.pdf.

Skoudis:2003:MFM

[SZ03] Ed Skoudis and Lenny Zeltser. *Malware: Fighting Malicious Code*. Prentice Hall series in computer networking and distributed systems. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 2003. ISBN 0-13-101405-6. 512 (est.) pp. LCCN QA76.9.A25 S58 2003. US$44.99.

Sarikaya:2008:SPT

[SZ08] Behcet Sarikaya and Xiao Zheng. SIP paging and tracking of wireless LAN hosts for VoIP. *IEEE/ACM Transactions on Networking*, 16(3):539–548, June 2008. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Sun:2002:NAD

[SZP02] Qi Sun, Qi Fan Zhang, and Guo Hua Peng. A new algorithm for the Dickson polynomial $g_e(x, 1)$ public key cryptosystem. *Sichuan Daxue Xuebao*, 39(1):18–23, 2002. CODEN SCTHAO. ISSN 0490-6756.

Sun:2005:WIW

[SZS05] Da-Zhi Sun, Ji-Dong Zhong, and Yu Sun. Weakness and improvement on Wang–Li–Tie's user-friendly remote authentication scheme. *Applied Mathematics and Computation*, 170(2):1185–1193, November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Tada:2002:OSM

[Tad02] Mitsuru Tada. An order-specified multisignature scheme secure against active insider attacks. *Lecture Notes in Computer Science*, 2384: 328–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/

link/service/series/0558/bibs/2384/23840328.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840328.pdf.

Tang:2001:AES

[Tan01] Ye Tang. The advanced encryption standard mapping into MorphoSys architecture. Thesis (M.S., Electrical and Computer Engineering), University of California, Irvine, Irvine, CA, USA, 2001.

Tang:2007:MMU

[Tan07a] Ping Tak Peter Tang. Modular multiplication using redundant digit division. In Kornerup and Muller [KM07], pages 217–224. ISBN 0-7695-2854-6. ISSN 1063-6889. LCCN ???? URL http://www.lirmm.fr/arith18/.

Tang:2007:SGK

[Tan07b] Qiang Tang. On the security of a group key agreement protocol. *The Computer Journal*, 50(5):589–590, September 2007. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/50/5/589; http://comjnl.oxfordjournals.org/cgi/content/full/50/5/589; http://comjnl.oxfordjournals.org/cgi/reprint/50/5/589.

Tattersall:2005:ENT

[Tat05] James J. (James Joseph) Tattersall. *Elementary number theory in nine chapters*. Cambridge University Press, Cambridge, UK, second edition, 2005. ISBN 0-521-85014-2 (hardcover), 0-521-61524-0 (paperback), 0-511-75634-8 (e-book). xi + 430 pp. LCCN ????

Trichina:2001:SCH

[TBDL01] Elena Trichina, Marco Bucci, Domenico De Seta, and Raimondo Luzzi. Supplemental cryptographic hardware for smart cards. *IEEE Micro*, 21(6):26–35, November/December 2001. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://dlib.computer.org/mi/books/mi2001/m6026abs.htm; http://dlib.computer.org/mi/books/mi2001/pdf/m6026.pdf.

Tistarelli:2002:BAI

[TBJ02] Massimo Tistarelli, Josef Bigun, and Anil K. Jain, editors. *Biometric authentication: International ECCV 2002 Workshop, Copenhagen, Denmark, June 1, 2002: Proceedings*, volume 2359 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9.

ISBN 3-540-43723-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.P3 I568 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2359.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2359.

Tao:2000:ITF

[TC00] Renji Tao and Shihua Chen. Input-trees of finite automata and application to cryptanalysis. *J. Comput. Sci. Tech.*, 15(4):305–325, 2000. CODEN JCTEEM. ISSN 1000-9000.

Tsai:2001:GSI

[TC01] Chwei-Shyong Tsai and Chin-Chen Chang. A generalized secret image sharing and recovery scheme. *Lecture Notes in Computer Science*, 2195:963–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950963.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950963.pdf.

Tsaur:2005:EAS

[TC05] Woei-Jiunn Tsaur and Chih-Ho Chou. Efficient algorithms for speeding up the computations of elliptic curve cryptosystems. *Applied Mathematics and Computation*, 168(2):1045–1064, September 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Tsai:2002:SMS

[TCC02] Chwei-Shyong Tsai, Chin-Chen Chang, and Tung-Shou Chen. Sharing multiple secrets in digital images. *The Journal of Systems and Software*, 64(2):163–170, November 15, 2002. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Trudel:2003:DSE

[TCR03] Bernard Trudel, Sean Convery, and Russell Rice. *Designing secure enterprise networks*. Cisco Press, Indianapolis, IN, USA, 2003. ISBN 1-58705-115-X. ???? pp. Duplicate ISBN with [Con04].

Teepe:2006:PPA

[Tee06] Wouter Teepe. Proving possession of arbitrary secrets while not giving them away: New protocols and a proof in GNY logic. *Synthese*, 149(2):409–443, March 2006. CODEN SYNTAE. ISSN 0039-7857 (print), 1573-0964 (electronic). URL http://link.springer.com//content/

pdf/10.1007/s11229-005-3879-4.pdf; http://link.springer.com/article/10.1007/s11229-005-3879-4.

Todd:2001:LSS

[TEM+01] Andrew W. Todd, Jonathan Erickson, Nadine McKenzie, Chris Cleeland, Richard Huang, Ragae Ghaly, and The Editors. Letters: Shared source and shared secrets; JavaScript fix; CORBA interoperability; EJB application servers update; correction ["The Delphi XML SAX2 Component and MSXML 3.0"]. *Dr. Dobb's Journal of Software Tools*, 26(10):10, 12, October 2001. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/. See [Hei01].

Terai:2008:BRB

[Ter08] S. Terai. Book review: *Cryptography in C and C++*, by Michael Welschenbach, Apress, 2005. *ACM SIGACT News*, 39(1):12–16, March 2008. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL http://doi.acm.org/10.1145/1360443.1360446. See [WK01, Wel05].

Thorsteinson:2004:NSC

[TG04] Peter Thorsteinson and G. Gnana Arun Ganesh. *.NET Security and Cryptography*. The integrated .NET series from object innovations. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 2004. ISBN 0-13-100851-X. xvii + 466 pp. LCCN ???? US$49.99.

Theoharidou:2007:CBK

[TG07] Marianthi Theoharidou and Dimitris Gritzalis. Common body of knowledge for information security. *IEEE Security & Privacy*, 5(2):64–67, March/April 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Tirkel:2001:UWE

[TH01] Andrew Z. Tirkel and Thomas E. Hall. A unique watermark for every image. *IEEE MultiMedia*, 8(4):30–37, October 2001. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://dlib.computer.org/mu/books/mu2001/pdf/u4030.pdf; http://www.computer.org/multimedia/mu2001/u4030abs.htm.

Thimbleby:2003:RE

[Thi03] Harold Thimbleby. The reduced Enigma. *Computers & Security*, 22(7):624–642, October 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803007120.

Tabatabaian:2001:NSP

[TIGD01] Seyed J. Tabatabaian, Sam Ikeshiro, Murat Gumussoy, and Mungal S. Dhanda. A new search pattern in multiple residue method (MRM) and its importance in the cryptanalysis of the RSA. *Lecture Notes in Computer Science*, 2260:378–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600378.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600378.pdf`.

Tippett:1927:RSN

[Tip27] L. H. C. (Leonard Henry Caleb) Tippett. *Random sampling numbers*, volume 15 of *Tracts for computers*. Cambridge University Press, Cambridge, UK, 1927. viii + xxvi pp. LCCN QA47 .T7 no. 15. Reprinted in 1952. Reprinted in 1959 with a foreword by Karl Pearson.

Torres:2007:ANS

[TIS07] Joaquin Torres, Antonio Izquierdo, and Jose Maria Sierra. Advances in network smart cards authentication. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(9):2249–2261, June 20, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Tseng:2001:GGO

[TJ01a] Y.-M. Tseng and J.-K. Jan. Generalized group-oriented cryptosystem with authenticated sender. *International Journal of Computer Systems Science and Engineering*, 16(5):??, September 2001. CODEN CSSEEI. ISSN 0267-6192.

Tseng:2001:CLB

[TJ01b] Yuh-Min Tseng and Jinn-Ke Jan. Cryptanalysis of Liaw's broadcasting cryptosystem. *Computers and Mathematics with Applications*, 41 (12):1575–1578, 2001. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Tseng:2003:DSM

[TJC03] Yuh-Min Tseng, Jinn-Ke Jan, and Hung-Yu Chien. Digital signature with message recovery using self-certified public keys and its variants. *Applied Mathematics and Computation*, 136 (2–3):203–214, March 15, 2003. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Tico:2003:RAS

[TK03] Marius Tico and Pauli Kuosmanen. A remote authentication system using fingerprints. *International Jour-*

nal of Image and Graphics (IJIG), 3(3):425–??, July 2003. CODEN ???? ISSN 0219-4678.

Toll:2008:CSE

[TKP+08] David C. Toll, Paul A. Karger, Elaine R. Palmer, Suzanne K. McIntosh, and Sam Weber. The Caernarvon secure embedded operating system. *Operating Systems Review*, 42(1):32–39, January 2008. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Thien:2002:TSS

[TL02] Chih-Ching Thien and Ja-Chen Lin. Technical section: Secret image sharing. *Computers and Graphics*, 26(5):765–770, October ??, 2002. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL `http://www.elsevier.com/gej-ng/10/13/20/68/56/39/abstract.html`.

Thomas:2007:HQU

[TL07] David B. Thomas and Wayne Luk. High quality uniform random number generation using LUT optimised state-transition matrices. *Journal of VLSI Signal Processing*, 47(1):77–92, 2007. CODEN JVSPED. ISSN 0922-5773. From the issue entitled “Special Issue: Field Programmable Technology. Guest Editors: Gordon Brebner, Samarjit Chakraborty, and Weng-Fai Wong”.

Turner:2006:SIS

[TLC06] Stephen John Turner, Bu Sung Lee, and Wientong Cai, editors. *Sixth International Symposium on Cluster Computing and the Grid CCGrid 06: 16–19 May, 2006, Singapore*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2006. ISBN 0-7695-2585-7. LCCN QA76.9.C58. IEEE Computer Society Order Number P2585.

Tsai:2005:CAE

[TLH05] Chwei-Shyong Tsai, Shu-Chen Lin, and Min-Shiang Hwang. Cryptanalysis of an authenticated encryption scheme using self-certified public keys. *Applied Mathematics and Computation*, 166(1):118–122, July 6, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Tan:2004:OBC

[TLYL04] Zhangxi Tan, Chuang Lin, Hao Yin, and Bo Li. Optimization and benchmark of cryptographic algorithms on network processors. *IEEE Micro*, 24(5):55–69, September/October 2004. CO-

DEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://csdl.computer.org/dl/mags/mi/2004/05/m5055.htm; http://csdl.computer.org/dl/mags/mi/2004/05/m5055.pdf.

Tokita:2001:ADC

[TM01] Toshio Tokita and Tsutomu Matsumoto. On applicability of differential cryptanalysis, linear cryptanalysis and mod n cryptanalysis to an encryption algorithm M8 (ISO9979-20). *IPSJ J.*, 42(8):2098–2105, 2001. ISSN 0387-5806.

Tang:2006:CHA

[TM06] Qiang Tang and Chris J. Mitchell. Cryptanalysis of a hybrid authentication protocol for large mobile networks. *The Journal of Systems and Software*, 79 (4):496–501, April 2006. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Torrubia:2001:CRC

[TMM01] Andres Torrubia, Francisco J. Mora, and Luis Marti. Cryptography regulations for e-commerce and digital rights management. *Computers & Security*, 20(8):724–738, December 1, 2001. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404801008148.

Tian:2005:RWS

[TMMM05] Junfeng Tian, Guofu Ma, Shengfu Ma, and Yahui Meng. Research on Web server attacking-based intrusion detection. In Han et al. [HYZ05b], pages 159–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Tsolis:2009:ARM

[TND+09] Dimitrios Tsolis, Spiridon Nikolopoulos, Lambros Drossos, Spyros Sioutas, and Theodore Papatheodorou. Applying robust multibit watermarks to digital images. *Journal of Computational and Applied Mathematics*, 227(1):213–220, May 1, 2009. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042708003543.

Teoh:2004:PCK

[TNG04] Andrew B. J. Teoh, David C. L. Ngo, and Alwyn Goh. Personalised cryptographic key generation based on FaceHashing. *Computers & Security*, 23(7):606–614, October 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001701.

Tousidou:2000:IMS

[TNM00] Eleni Tousidou, Alex Nanopoulos, and Yannis Manolopoulos. Improved methods for signature-tree construction. *The Computer Journal*, 43(4):301–314, ???? 2000. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_43/Issue_04/430301.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_43/Issue_04/pdf/430301.pdf.

Tanaka:2001:QPK

[TO01] Keisuke Tanaka and Tatsuaki Okamoto. Quantum public-key cryptosystems and their improvement. *Sūrikaisekikenkyūsho Kōkyūroku*, 1205:53–58, 2001. New developments of the theory of computation and algorithms (Japanese) (Kyoto, 2001).

Tochikubo:2000:RAE

[TOEO00] Kouya Tochikubo, Koji Okada, Naoki Endoh, and Eiji Okamoto. Renewable authentication and encryption systems. *Transactions of the Information Processing Society of Japan*, 41(8):2121–2127, 2000. CODEN JSGRD5. ISSN 0387-5806.

Tomaszewski:2006:YSY

[Tom06] John P. Tomaszewski. Are you sure you had a privacy incident? *IEEE Security & Privacy*, 4(6):64–66, November/December 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Topham:2002:BRJ

[Top02] Jon Topham. Book review: James A. Secord, Victorian Sensation: The Extraordinary Publication, Reception, and Secret Authorship of Vestiges of the Natural History of Creation. Chicago and London: University of Chicago Press, 2001. Pp. xix + 624. ISBN 0-226-74410-8. £22.50, $35.00 (hardcover). *British Journal for the History of Science*, 35(3):347–379, September 2002. CODEN BJHSAT. ISSN 0007-0874 (print), 1474-001X (electronic).

Totsch:2000:MSS

[Tot00] David Totsch. Managing SUID/SGID files. *Sys Admin: The Journal for UNIX Systems Administrators*, 9(9):60, 62–63, 65, September 2000. CODEN SYADE7. ISSN 1061-2688. URL http://www.samag.com/.

Tague:2007:CSA

[TP07] Patrick Tague and Radha Poovendran. A canonical seed assignment model for key predistribution in wireless sensor networks. *ACM Transactions on Sensor Networks*, 3(4):19:1–19:??, October 2007. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Trope:2007:CSD

[TPPM07] Roland L. Trope, E. Michael Power, Vincent I. Polley, and Bradford C. Morley. A coherent strategy for data security through data governance. *IEEE Security & Privacy*, 5(3):32–39, May/June 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Trimberger:2001:GED

[TPS01] Steve Trimberger, Raymond Pang, and Amit Singh. A 12 Gbps DES encryptor/decryptor core in an FPGA. *Lecture Notes in Computer Science*, 1965: 156–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1965/19650156.htm; http://link.springer-ny.com/link/service/series/0558/papers/1965/19650156.pdf`.

Troutman:2009:CCGa

[TR09a] Justin Troutman and Vincent Rijmen. Crypto corner: Green cryptography: Cleaner engineering through recycling. *IEEE Security & Privacy*, 7(4):71–73, July/August 2009. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Troutman:2009:CCGb

[TR09b] Justin Troutman and Vincent Rijmen. Crypto corner: Green cryptography: Cleaner engineering through recycling, part 2. *IEEE Security & Privacy*, 7(5): 64–65, September/October 2009. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Troutman:2008:VMM

[Tro08] Justin Troutman. The virtues of mature and minimalist cryptography. *IEEE Security & Privacy*, 6(4):62–65, July/August 2008. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Tsaur:2001:FUA

[Tsa01] W.-J. Tsaur. A flexible user authentication scheme for multi-server Internet services. *Lecture Notes in Computer Science*, 2093: 174–??, 2001. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2093/20930174.htm; http://link.springer-ny.com/link/service/series/0558/papers/2093/20930174.pdf.

Tsaur:2005:SSS

[Tsa05] Woei-Jiunn Tsaur. Several security schemes constructed using ECC-based self-certified public key cryptosystems. *Applied Mathematics and Computation*, 168(1):447–464, September 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Tsaban:2006:FGD

[Tsa06] Boaz Tsaban. Fast generators for the Diffie–Hellman key agreement protocol and malicious standards. *Information Processing Letters*, 99(4):145–148, August 31, 2006. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Tsang:2007:WCT

[Tsa07] Patrick P. Tsang. When cryptographers turn lead into gold. *IEEE Security & Privacy*, 5(2):76–79, March/April 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Tsai:2008:EMS

[Tsa08] Jia-Lun Tsai. Efficient multi-server authentication scheme based on one-way hash function without verification table. *Computers & Security*, 27(3–4):115–121, May/June 2008. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808000084.

Tseng:2007:SAG

[Tse07] Yuh-Min Tseng. A secure authenticated group key agreement protocol for resource-limited mobile devices. *The Computer Journal*, 50(1):41–52, January 2007. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/50/1/41; http://comjnl.oxfordjournals.org/cgi/content/full/50/1/41; http://comjnl.oxfordjournals.org/cgi/reprint/50/1/41.

Takano:2000:PTH

[TSO00] Kohji Takano, Akashi Satoh, and Nobuyuki Ohba. Poster 5: TATSU — hardware accelerator for public-key cryptography using Montgomery method. In Anonymous [Ano00d], page ??

Tsunoo:2003:CIC

[TSS+03] Yukiyasu Tsunoo, Teruo Saito, Tomoyasu Suzaki, Maki Shigeri, and Hiroshi Miyauchi. Cryptanalysis of DES implemented on computers with cache. In Walter et al. [WKP03], pages 62–76. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Tahir:2000:RCM

[TT00] Farasat Tahir and Muhammad Tahir. RSA ciphers with Maple. *Punjab Univ. J. Math. (Lahore)*, 33:145–152, 2000. ISSN 1016-2526.

Tzeng:2001:PKT

[TT01] Wen-Guey Tzeng and Zhi-Jia Tzeng. A public-key traitor tracing scheme with revocation using dynamic shares. *Lecture Notes in Computer Science*, 1992: 207–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920207.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920207.pdf.

Tian:2001:ICE

[TTZ01] Jun Tian, Tieniu Tan, and Liangpei Zhang, editors. *Image compression and encryption technologies: 22–24 October 2001, Wuhan, China*, volume 4551 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 2001. ISBN 0-8194-4279-8. LCCN TK5105.59 .I43 2001.

Tuchman:1966:ZT

[Tuc66] Barbara W. Tuchman. *The Zimmermann telegram.* MacMillan Publishing Company, New York, NY, USA, 1966. xii + 244 pp. LCCN D511 .T77 1966. Reprint of original 1958 edition. Kahn [Kah96] describes this book as "recount[ing] the political effects of the most important cryptogram solution in history".

Turing:2004:BS

[Tur04] Alan M. Turing. Bombe and Spider. In Copeland [Cop04b], pages 313–335. ISBN 0-19-825079-7 (hardcover), 0-19-825080-0 (paperback). LCCN QA29.T8

E77 2004. URL ftp://uiarchive.cso.uiuc.edu/pub/etext/gutenberg/; http://www.loc.gov/catdir/toc/fy053/2004275594.html. Text prepared by Ralph Erskine and Philip Marks and Frode Weierud from the only two surviving copies of Turing's typescript.

Tiri:2003:SEA

[TV03] Kris Tiri and Ingrid Verbauwhede. Securing encryption algorithms against DPA at the logic level: Next generation Smart Card technology. In Walter et al. [WKP03], pages 125–136. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Toft:2001:LTT

[TvdKB+01] George Toft, Hugo van der Kooij, Mick Bauer, Chris Hendrickson, Stephanie Black, Adrian Ho, Markus Hogger, Ian Abbott, and Robin Rowes. Letters: Tech tipsy; awkward solution; Mandrake 7.2 review; OpenSSH and DSA keys; missed the tripwire; FAT problems. *Linux Journal*, 85:6, 126, May 2001. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://noframes.linuxjournal.com/lj-issues/issue85/4646.html.

Trappe:2002:ICC

[TW02] Wade Trappe and Lawrence C. Washington. *Introduction to Cryptography with Coding Theory*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 2002. ISBN 0-13-061814-4. xiii + 490 pp. LCCN QA268 .T73 2002. UK£29.99.

Trappe:2005:ICC

[TW05] Wade Trappe and Lawrence C. Washington. *Introduction to cryptography: with coding theory*. Pearson Prentice Hall, Upper Saddle River, NJ, USA, second edition, 2005. ISBN 0-13-186239-1. xiv + 577 pp. LCCN QA268 .T73 2005.

Talbot:2006:CCI

[TW06a] J. (John) Talbot and D. J. A. Welsh. *Cryptography and complexity: an introduction*. Cambridge University Press, Cambridge, UK, 2006. ISBN 0-521-85231-5 (hardcover), 0-521-61771-5 (paperback). xii + 292 pp. LCCN Z103 .T35 2006.

Trappe:2006:ICC

[TW06b] Wade Trappe and Lawrence C. Washington. *Introduction to Cryptography: with Coding Theory*. Pearson Prentice Hall, Upper Saddle River, NJ, USA, second edition, 2006. ISBN 0-13-186239-1, 0-13-198199-4 (paperback). xiv + 577 pp. LCCN QA268 .T73 2006.

Tsai:2007:TTA

[TW07] Yuh-Ren Tsai and Shiuh-Jeng Wang. Two-tier authentication for cluster and individual sets in mobile ad hoc networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 51(3):883–900, February 21, 2007. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Tsaur:2005:EUA

[TWL05] Woei-Jiunn Tsaur, Chia-Chun Wu, and Wei-Bin Lee. An enhanced user authentication scheme for multi-server Internet services. *Applied Mathematics and Computation*, 170(1): 258–266, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Tiwari:2009:CIF

[TWM+09] Mohit Tiwari, Hassan M. G. Wassel, Bita Mazloom, Shashidhar Mysore, Frederic T. Chong, and Timothy Sherwood. Complete information flow tracking from the gates up. *ACM SIGPLAN Notices*, 44(3):109–120, March 2009. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Thamrin:2008:PBR

[TWNA08] N. M. Thamrin, G. Witjaksono, A. Nuruddin, and M. S. Abdullah. A photonic-based random number generator for cryptographic application. In *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2008. SNPD '08*, pages 356–361. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4617397`.

Tzeng:2004:NTM

[TYH04] Shiang-Feng Tzeng, Cheng-Ying Yang, and Min-Shiang Hwang. A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. *Future Generation Computer Systems*, 20(5):887–893, June 15, 2004. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Ting:2002:FBS

[TYLL02] Kurt K. Ting, Steve C. L. Yuen, K. H. Lee, and Philip H. W. Leong. An FPGA based SHA-256 processor. *Lecture Notes in Computer Science*, 2438: 577–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2438/24380577.htm; http://link.springer-ny.com/link/service/series/0558/papers/2438/24380577.pdf.

Tynan:2005:CPA

[Tyn05] Dan Tynan. *Computer privacy annoyances: how to avoid the most annoying invasions of your personal and online privacy*. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, USA, 2005. ISBN 0-596-00775-2 (paperback). xii + 177 pp. LCCN QA76.9.A25 T96 2005.

Tian:2005:NDF

[TZDZ05] Junfeng Tian, Weidong Zhao, Ruizhong Du, and Zhe Zhang. A new data fusion model of intrusion detection—IDSFM. In Han et al. [HYZ05b], pages 73–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Tong:2009:RAPa

[TZT09a] Qiaoling Tong, Xuecheng Zou, and Hengqing Tong. A RFID authentication protocol based on infinite dimension pseudo random number generator. In *2009. CSO 2009. International Joint Conference on Computational Sciences and Optimization*, volume 1, pages 292–294. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5193698.

Tong:2009:RAPb

[TZT09b] Qiaoling Tong, Xuecheng Zou, and Hengqing Tong. A RFID authentication protocol based on infinite dimension pseudo random number generator for face recognition system. In *2009. ICBBE 2009. 3rd International Conference on Bioinformatics and Biomedical Engineering*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5162237.

Uz:2009:MBT

[UBEP09] Tamer Uz, George Bebis, Ali Erol, and Salil Prabhakar. Minutiae-based template synthesis and matching for fingerprint authentication. *Computer Vision and Image Understanding: CVIU*, 113(9):979–992, September 2009. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic).

Unay:2008:SQE

[ÜG08] Ozan Ünay and Taflan I. Gündem. A survey on querying encrypted XML documents for databases as a service. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 37(1):12–20, March 2008. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Uchida:2009:FPR

[UHA+09] A. Uchida, T. Honjo, K. Amano, K. Hirano, H. Someya, H. Okumura, S. Yoshimori, K. Yoshimura, P. Davis, and Y. Tokura. Fast physical random bit generator based on chaotic semiconductor lasers: Application to quantum cryptography. In *Lasers and Electro-Optics 2009 and the European Quantum Electronics Conference. CLEO Europe - EQEC 2009. European Conference on*, page 1. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5192510`.

USC:2000:HRS

[Uni00a] United States Congress. *H.R. 850, the Security and Freedom through Encryption (SAFE) Act: Markup before the Committee on International Relations, House of Representatives, One Hundred Sixth Congress, first session, Tuesday, July 13, 1999.* United States Government Printing Office, Washington, DC, USA, 2000. ISBN 0-16-060340-4, 0-16-060340-4. iii + 102 pp. LCCN KF27.I53 106th.

USHCAS:2000:UEP

[Uni00b] United States Congress.House Committee on Armed Services. *U.S. encryption policy: hearing before the Committee on Armed Services, House of Representatives, One Hundred Sixth Congress, first session: hearings held July 1, 13, 1999.* Washington, DC, USA, 2000. iv + 195 pp. H.A.S.C. no. 106-16.

USHCIR:2000:HES

[Uni00c] United States Congress.House Committee on International

Relations. *106-1 Hearing: Encryption Security in a High Tech Era, May 18, 1999*. Washington, DC, USA, 2000. Shipping List #: 2000-0319-P. Shipping List Date: 07/31/2000.

USHCIR:2000:MHS

[Uni00d] United States Congress.House Committee on International Relations. *106-1 Markup: H.R. 850, The Security And Freedom Through Encryption (SAFE) Act, July 13, 1999*. Washington, DC, USA, 2000. Shipping List #: 2000-0214-P. Shipping List Date: 04/20/2000.

USHCIR:2000:HSF

[Uni00e] United States Congress.House Committee on International Relations. *H.R. 850, the Security and Freedom through Encryption (SAFE) Act: markup before the Committee on International Relations, House of Representatives, One Hundred Sixth Congress, first session, Tuesday, July 13, 1999*. Washington, DC, USA, 2000. iii + 102 pp. Shipping list no.: 2000-0214-P.

USHCIR:2000:ESH

[Uni00f] United States Congress.House Committee on International Relations.Subcommittee on International Economic Policy and Trade. *Encryption security in a high tech era: hearing before the Subcommittee on International Economic Policy and Trade of the Committee on International Relations, House of Representatives, One Hundred Sixth Congress, first session, Tuesday, May 18, 1999*. Washington, DC, USA, 2000. iii + 60 pp. Serial no. 106-108. Shipping list no.: 2000-0319-P.

USHCJ:2000:HSF

[Uni00g] United States Congress.House Committee on the Judiciary. *106-1 Hearing: Security And Freedom Through Encryption, (SAFE) Act, Serial No. 34, March 4, 1999*. Washington, DC, USA, 2000. Shipping List #: 2000-0275-P. Shipping List Date: 06/21/2000.

USHCJ:2000:SFT

[Uni00h] United States Congress.House Committee on the Judiciary.Subcommittee on Courts and Intellectual Property. *Security and Freedom through Encryption (SAFE) Act: hearing before the Subcommittee on Courts and Intellectual Property of the Committee on the Judiciary, House of Representatives, One Hundred Sixth Congress, first session, on H.R. 850, March 4, 1999*. Washington, DC, USA, 2000. iv + 169 pp. Serial no. 34. Shipping list no.: 2000-0275-P.

USPTO:2001:CCP

[Uni01] United States Patent and Trademark Office. *Class 380 — Cryptography, Patent Classification Definitions, Patent and Trademark Office, U.S. Dept. of Commerce, December 1999.* Washington, DC, USA, 2001. Shipping List #: 2001-0468-M. Shipping List Date: 08/31/2001.

Uhl:2005:IVE

[UP05] Andreas Uhl and Andreas Pommer. *Image and video encryption: from digital rights management to secured personal communication*, volume 15 of *Advances in information security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 0-387-23402-0. xvi + 161 pp. LCCN TA1637 .U72 2005.

Urban:2001:MWB

[Urb01] Mark Urban. *The Man Who Broke Napoleon's Codes.* Faber and Faber, London, UK, 2001. ISBN 0-571-20513-5. xiv + 333 pp. LCCN DC232.U73 2001. UK£16.99.

Urien:2001:PIS

[Uri01] Pascal Urien. Programming Internet smartcard with XML scripts. *Lecture Notes in Computer Science*, 2140:228–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400228.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2140/21400228.pdf`.

USENIX:2000:PLI

[USE00a] USENIX, editor. *Proceedings of the 3rd Large Installation System Administration of Windows NT/2000 Conference: August 1–2, 2000, Seattle, Washington, USA*. USENIX, Berkeley, CA, USA, 2000. ISBN 1-880446-19-7. LCCN ???? URL `http://db.usenix.org/publications/library/proceedings/lisa-nt2000/`.

USENIX:2000:PFW

[USE00b] USENIX, editor. *Proceedings of the First Workshop on Industrial Experiences with Systems Software (WIESS 2000), October 22, 2000, Paradise Point Resort, San Diego, California, USA*. USENIX, Berkeley, CA, USA, 2000. ISBN 1-880446-15-4. LCCN QA76.76.S95 W67 2000. URL `http://www.usenix.org/publications/library/proceedings/osdi2000/wiess2000/`.

USENIX:2000:PFSa

[USE00c] USENIX, editor. *Proceedings of the Fourteenth Systems Administration Conference (LISA XIV), December 3–8, 2000, New Orleans, Louisiana, USA*. USENIX, Berkeley, CA, USA, 2000. ISBN 1-880446-13-8. LCCN ???? URL `http://www.usenix.org/publications/library/proceedings/lisa2000/technical.html`.

USENIX:2000:PNU

[USE00d] USENIX, editor. *Proceedings of the Ninth USENIX Security Symposium, August 14–17, 2000, Denver, Colorado*. USENIX, Berkeley, CA, USA, 2000. ISBN 1-880446-18-9. LCCN ???? URL `http://www.usenix.org/publications/library/proceedings/sec2000`.

USENIX:2001:PUA

[USE01a] USENIX, editor. *Proceedings of the 2001 USENIX Annual Technical Conference: June 25–30, 2001, Marriott Copley Place Hotel, Boston, Massachusetts, USA*. USENIX, Berkeley, CA, USA, 2001. ISBN 1-880446-09-X. LCCN QA76.8.U65 U84 2001. URL `http://www.usenix.org/publications/library/proceedings/usenix01/technical.html`.

USENIX:2001:PFT

[USE01b] USENIX, editor. *Proceedings of the FREENIX Track: 2001 USENIX Annual Technical Conference: June 25–30, 2001, Marriott Copley Place Hotel, Boston, Massachusetts, USA*. USENIX, Berkeley, CA, USA, 2001. ISBN 1-880446-10-3. LCCN QA76.8.U65 U84 2001. URL `http://www.usenix.org/publications/library/proceedings/usenix01/freenix01/technical.html`.

USENIX:2001:PTU

[USE01c] USENIX, editor. *Proceedings of the Tenth USENIX Security Symposium, August 13–17, 2001, Washington, DC, USA*. USENIX, Berkeley, CA, USA, 2001. ISBN 1-880446-18-9, 1-880446-07-3. LCCN QA76.9.A25 U565 2001. URL `http://www.usenix.org/publications/library/proceedings/sec01/technical.html`.

USENIX:2002:PBF

[USE02a] USENIX, editor. *Proceedings of BSDCon 2002: February 11–14, 2002, Cathedral Hill Hotel, San Francisco, CA*. USENIX, Berkeley, CA, USA, 2002. ISBN 1-880446-02-2. LCCN QA76.76.O63 B736 2002. URL `http://www.usenix.org/publications/library/proceedings/bsdcon02/tech.html`.

USENIX:2002:PUS

[USE02b] USENIX, editor. *Proceed-*

ings of the 11th USENIX Security Symposium 2002, August 5–9, 2002, San Francisco, CA. USENIX, Berkeley, CA, USA, 2002. ISBN 1-931971-00-5. LCCN ???? URL `http://www.usenix.org/publications/library/proceedings/sec02/`.

USENIX:2002:PFT

[USE02c] USENIX, editor. *Proceedings of the FREENIX Track: 2002 USENIX Annual Technical Conference, June 10–15, 2002, Monterey, California, USA*. USENIX, Berkeley, CA, USA, 2002. ISBN 1-880446-01-4. LCCN QA76.8.U65 P765 2002. URL `http://www.usenix.org/publications/library/proceedings/usenix02/`.

Utami:2002:FID

[USS02] Dewi Utami, Hadi Suwastio, and Bambang Sumadjudin. FPGA implementation of digital chaotic cryptography. *Lecture Notes in Computer Science*, 2510: 239–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2510/25100239.htm`; `http://link.springer.de/link/service/series/0558/papers/2510/25100239.pdf`.

Urien:2001:XS

[UST01a] P. Urien, H. Saleh, and A. Tizraoui. XML smartcards. *Lecture Notes in Computer Science*, 2093: 811–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2093/20930811.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2093/20930811.pdf`.

Ustimenko:2001:CGT

[Ust01b] Vasyl Ustimenko. CRYPTIM: Graphs as tools for symmetric encryption. In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 278–286. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL `http://link.springer-ny.com/link/service/series/0558/bibs/2227/22270278.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2227/22270278.pdf`.

Ulfving:2000:GS

[UW00] Lars Ulfving and Frode Weierud. The Geheimschreiber secret. In Joyner

[Joy00], page ?? ISBN 3-540-66336-3 (softcover), 3-642-59663-0 (e-book). LCCN QA268 .C67 1999. UK£44.50. URL http://frode.home.cern.ch/frode/pubs/cryptoday.pdf. Proceedings of the Conference on Coding Theory, Cryptography and Number Theory held at the U.S. Naval Academy during October 25–26, 1998.

Uzun:2004:BRC

[Uzu04] Isa Servan Uzun. Book review: *Cryptographic Security Architecture—Design and Verification*, by Peter Gutmann. *The Computer Journal*, 47(5):622–623, September 2004. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/free_pdf/470622a.pdf; http://www3.oup.co.uk/computer_journal/hdb/Volume_47/Issue_05/470622a.sgm.abs.html.

Vacca:2006:GWN

[Vac06] John R. Vacca. *Guide to wireless network security*, volume 20 of *Advances in information security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 0-387-95425-2. xxii + 848 pp. LCCN QA76.9.A25 C66 2006. URL http://www.loc.gov/catdir/enhancements/fy0663/2005939009-d.html.

Vadhan:2003:CLC

[Vad03] Salil P. Vadhan. On constructing locally computable extractors and cryptosystems in the bounded storage model. In Boneh [Bon03], pages 61–77. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2729.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11817.

Vanstone:2003:NGS

[Van03] S. A. Vanstone. Next generation security for wireless: elliptic curve cryptography. *Computers & Security*, 22(5):412–415, July 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803005078.

Vaudenay:2001:DID

[Vau01] Serge Vaudenay. Decorrelation over infinite domains: The encrypted CBC–MAC case. *Lecture Notes in*

Computer Science, 2012: 189–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120189.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120189.pdf.

Vaudenay:2002:SFI

[Vau02] Serge Vaudenay. Security flaws induced by CBC padding — applications to SSL, IPSEC, WTLS .... *Lecture Notes in Computer Science*, 2332: 534–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320534.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320534.pdf.

Vaudenay:2005:PKC

[Vau05a] Serge Vaudenay, editor. *Public key cryptography — PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23–26, 2005: Proceedings*, volume 3386 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-24454-9 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I567 2005. URL http://springerlink.metapress.com/openurl.asp?genre=issue&issn=0302-9743&volume=3386; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3386; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b105124.

Vaudenay:2005:SCI

[Vau05b] Serge Vaudenay. Secure communications over insecure channels based on short authenticated strings. In Shoup [Sho05a], pages 309–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Vavriv:2003:RNG

[Vav03] D. D. Vavriv. Random number generators on the basis of systems with chaotic behavior. *AIP*

Conference Proceedings, 676 (1):373, 2003. CODEN APCPCS. ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. URL `http://link.aip.org/link/?APC/676/373/1`.

Vlachos:2009:OPV

[VAVY09] Michail Vlachos, Aris Anagnostopoulos, Olivier Verscheure, and Philip S. Yu. Online pairing of VoIP conversations. *VLDB Journal: Very Large Data Bases*, 18(1):77–98, January 2009. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Voloshynovskiy:2005:ITD

[VDKP05] Sviatoslav Voloshynovskiy, Frederic Deguillaume, Oleksiy Koval, and Thierry Pun. Information-theoretic data-hiding: Recent achievements and open problems. *International Journal of Image and Graphics (IJIG)*, 5 (1):5–??, January 2005. CODEN ???? ISSN 0219-4678.

vanDijk:2006:ICS

[vDKST06] Marten van Dijk, Tom Kevenaar, Geert-Jan Schrijen, and Pim Tuyls. Improved constructions of secret sharing schemes by applying (λ, ω)-decompositions. *Information Processing Letters*, 99(4):154–157, August 31, 2006. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

vanDijk:2004:AOC

[vDW04] Marten van Dijk and David Woodruff. Asymptotically optimal communication for torus-based cryptography. In Franklin [Fra04], pages 157–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099`.

Verheul:2001:EXM

[Ver01] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 2045:195–210, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vercauteren:2002:CZF

[Ver02] Frederik Vercauteren. Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2. In Yung [Yun02a], pages 369–384. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25

C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420369.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420369.pdf.

Vergnaud:2006:RBS

[Ver06a] Damien Vergnaud. RSA-based secret handshakes. In Ytrehus [Ytr06], pages 252–274. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Vernitski:2006:CUM

[Ver06b] Alexei Vernitski. Can unbreakable mean incomputable? *The Computer Journal*, 49(1):108–112, January 2006. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/49/1/108; http://comjnl.oxfordjournals.org/cgi/content/full/49/1/108; http://comjnl.oxfordjournals.org/cgi/reprint/49/1/108.

Vladimirov:2004:WFS

[VGM04] Andrew A. Vladimirov, Konstantin V. Gavrilenko, and Andrei A. Mikhailovsky. *Wi-Foo: The Secrets of Wireless Hacking*. Addison-Wesley, Reading, MA, USA, 2004. ISBN 0-321-20217-1. xxvii + 555 pp. LCCN TK5105.59 .V53 2004. URL http://www.awprofessional.com/title/0321202171.

Vassev:2009:STA

[VH09] Emil Vassev and Mike Hinchey. Software technologies: ASSL: a software engineering approach to autonomic computing. *Computer*, 42(6):90–93, June 2009. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Voloshynovskiy:2001:BDA

[VHP01] Sviatoslav Voloshynovskiy, Alexander Herrigel, and Thierry Pun. Blur/deblur attack against document protection systems based on digital watermarking. *Lecture Notes in Computer Science*, 2137: 330–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370330.htm; http://link.springer-ny.com/link/service/series/0558/papers/2137/21370330.pdf.

Viroli:2003:TPA

[Vir03] Mirko Viroli. A type-passing approach for the implementation of parametric methods in Java. *The Computer Journal*, 46(3): 263–294, May 2003. CO-

DEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_46/Issue_03/460263.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_46/Issue_03/pdf/460263.pdf.

Vixie:2002:SRR

[Vix02] Paul A. Vixie. Spam — roles and responsibilities, 2002. URL http://www.usenix.org/publications/library/proceedings/bsdcon02/tech.html. Unpublished invited talk, BSDCON2002: Growing the BSD Community, February 11–14, 2002, Cathedral Hill Hotel, San Francisco, CA.

Vural:2007:IND

[VK07] Cabir Vural and Serap Kazan. Image normalization and discrete wavelet transform based robust digital image watermarking. In Simos and Maroulis [SM07b], pages 1404–1407. ISBN 0-7354-0476-3 (set), 0-7354-0477-1 (vol. 1), 0-7354-0478-X (vol. 2). ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. LCCN Q183.9 .I524 2007. URL http://proceedings.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf& id=APCPCS000963000002001404000001& idtype=cvips.

Vo:2008:SMA

[VK08] Duc-Liem Vo and Kwangjo Kim. A secure mutual authentication scheme with key agreement using smart card from bilinear pairings. *International Journal of Computer Systems Science and Engineering*, 23 (3):??, May 2008. CODEN CSSEEI. ISSN 0267-6192.

Volos:2009:IEP

[VKS09] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos. Image encryption process based on a chaotic True Random Bit Generator. In *2009 16th International Conference on Digital Signal Processing*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5201107.

Viega:2003:SPC

[VM03] John Viega and Matt Messier. *Secure programming cookbook for C and C++: Recipes for cryptography, authentication, networking, input validation and more*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707

829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, 2003. ISBN 0-596-00394-3. xxv + 762 pp. LCCN QA76.73.C15 V53 2003.

Viega:2002:NSO

[VMC02] John Viega, Matt Messier, and Pravir Chandra. *Network Security with OpenSSL: Cryptography for Secure Communications*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, 2002. ISBN 0-596-00270-X. xiv + 367 pp. LCCN TK5105.59 .V54 2002. US$39.95. URL `http://safari.oreilly.com/059600270X`; `http://www.oreilly.com/catalog/openssl`.

Vasco:2005:NCS

[VMSV05] María Isabel González Vasco, Consuelo Martínez, Rainer Steinwandt, and Jorge L. Villar. A new Cramer–Shoup like methodology for group based provably secure encryption schemes. In Kilian [Kil05], pages 495–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171`.

Vaughan-Nichols:2004:VAS

[VN04] Steven J. Vaughan-Nichols. Voice authentication speaks to the marketplace. *Computer*, 37(3):13–??, March 2004. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://csdl.computer.org/dl/mags/co/2004/03/r3013.htm`; `http://csdl.computer.org/dl/mags/co/2004/03/r3013.pdf`.

Voice:2005:OAM

[Voi05] Chris Voice. Online authentication: matching security levels to the risk. *Network Security*, 2005(12):15–18, December 2005. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485805703159`.

vanOorschot:2008:PMU

[vOT08] P. C. van Oorschot and Julie Thorpe. On predictive models and user-drawn graphical passwords. *ACM Transactions on Information and System Security*, 10(4):5:1–5:??, January 2008. CODEN

ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

vanOorschot:2007:IRS

[vOWK07] P. C. van Oorschot, Tao Wan, and Evangelos Kranakis. On interdomain routing security and pretty secure BGP (psBGP). *ACM Transactions on Information and System Security*, 10(3):11:1–11:??, July 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Vogt:2001:USC

[VPG01] Holger Vogt, Henning Pagnia, and Felix C. Gärtner. Using smart cards for fair exchange. *Lecture Notes in Computer Science*, 2232: 101–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2232/22320101.htm; http://link.springer-ny.com/link/service/series/0558/papers/2232/22320101.pdf.

Vasco:2001:CPK

[VS01] María Isabel González Vasco and Rainer Steinwandt. Clouds over a public key cryptosystem based on Lyndon words. *Information Processing Letters*, 80(5):239–242, December 15, 2001. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.com/gej-ng/10/23/20/84/36/30/abstract.html.

Voyiatzis:2008:SFS

[VS08] Artemios G. Voyiatzis and Dimitrios N. Serpanos. The security of the Fiat–Shamir scheme in the presence of transient hardware faults. *ACM Transactions on Embedded Computing Systems*, 7(3):31:1–31:??, April 2008. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

vanTilborg:2000:FCP

[vT00] Henk C. A. van Tilborg. *Fundamentals of cryptology: a professional reference and interactive tutorial*, volume SECS 528 of *The Kluwer international series in engineering and computer science*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2000. ISBN 0-7923-8675-2. xiv + 490 pp. LCCN QA76.9.A25 T53 2000 Accompanying CD-Rom shelved in Reserves.

vanTilborg:2001:ECC

[vT01] Henk van Tilborg. Elliptic curve cryptosystems; too good to be true? *Nieuw Arch. Wiskd. (5)*, 2(3):220–225, 2001. ISSN 0028-9825.

vanTilborg:2005:ECS

[vT05] Henk C. A. van Tilborg, editor. *Encyclopedia of cryptography and security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 0-387-23473-X (hardcover). x + 684 pp. LCCN Z103 .E53 2005. US$299.00.

Vaudenay:2007:POK

[VV07] Serge Vaudenay and Martin Vuagnoux. Passive-only key recovery attacks on RC4. In Carlisle Adams, Ali Miri, and Michael Wiener, editors, *Selected areas in cryptography: 14th international workshop, SAC 2007, Ottawa, Canada, August 16–17, 2007, revised selected papers*, volume 4876 of *Lecture Notes in Computer Science*, pages 344–359. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-77359-2 (softcover). LCCN QA76.9 2007. URL `http://www.loc.gov/catdir/enhancements/fy0826/2007941250-d.html`.

Venkatesan:2001:GTA

[VVS01] Ramarathnam Venkatesan, Vijay Vazirani, and Saurabh Sinha. A graph theoretic approach to software watermarking. *Lecture Notes in Computer Science*, 2137: 157–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370157.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2137/21370157.pdf`.

vonWillich:2001:TIT

[vW01] Manfred von Willich. A technique with an information-theoretic basis for protecting secret data from differential power attacks. *Lecture Notes in Computer Science*, 2260:44–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600044.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2260/22600044.pdf`.

Vaudenay:2001:SAC

[VY01] Serge Vaudenay and Amr M. Youssef, editors. *Selected Areas in Cryptography: 8th Annual International Workshop, SAC 2001, Toronto, Ontario, Canada, August 16–17, 20001: proceedings*, volume 2259 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 3-540-43066-0. LCCN QA76.9.A25 S22 2001.

Whittaker:2006:HBW

[WA06] James A. Whittaker and Mike Andrews. *How to break Web software: functional and security testing of Web applications and Web services*. Addison-Wesley, Reading, MA, USA, 2006. ISBN 0-321-36944-0 (paperback). ???? pp. LCCN QA76.76.T48 W485 2006. URL http://www.loc.gov/catdir/toc/ecip064/2005034913.html.

Woody:2007:COS

[WA07] Carol Woody and Christopher Alberts. Considering operational security risk during system development. *IEEE Security & Privacy*, 5(1):30–35, January/February 2007. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Weitzner:2008:IA

[WABL+08] Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler, and Gerald Jay Sussman. Information accountability. *Communications of the Association for Computing Machinery*, 51 (6):82–87, June 2008. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Wachsmann:2005:CAK

[Wac05] Alf Wachsmann. Centralized authentication with Kerberos 5, Part I. *Linux Journal*, 2005(130):6, February 2005. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Wallach:2000:SSM

[WAF00] Dan S. Wallach, Andrew W. Appel, and Edward W. Felten. SAFKASI: a security mechanism for language-based systems. *ACM Transactions on Software Engineering and Methodology*, 9(4):341–378, October 2000. CODEN ATSMER. ISSN 1049-331X (print), 1557-7392 (electronic). URL http://www.acm.org/pubs/articles/journals/tosem/2000-9-4/p341-wallach/p341-wallach.pdf; http://www.acm.org/pubs/citations/journals/tosem/2000-9-4/p341-wallach/.

Wagner:2000:CYL

[Wag00] David Wagner. Cryptanalysis of the Yi-Lam hash. *Lecture Notes in Computer Science*, 1976:483–488, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wagner:2002:GBP

[Wag02] David Wagner. A generalized birthday problem: (extended abstract). In Yung [Yun02a], pages 288–303. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Wagstaff:2003:CNT

[Wag03] Samuel S. Wagstaff, Jr. *Cryptanalysis of number theoretic ciphers*. Computational mathematics. Chapman and Hall/CRC, Boca Raton, FL, USA, 2003. ISBN 1-58488-153-4. xv + 318 pp. LCCN QA76.9.A25 W33 2003. URL http://www.loc.gov/catdir/enhancements/fy0646/2002034919-d.html.

Walsh:2000:BRM

[Wal00] Gary Walsh. Book review: *The Mathematics of Ciphers, Number Theory and RSA Cryptography*. *Mathematics of Computation*, 69(231):1314–1315, July 2000. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2000-69-231/S0025-5718-00-01249-7/bookrev-S0025-5718-00-01249-7.html; http://www.ams.org/mcom/2000-69-231/S0025-5718-00-01249-7/S0025-5718-00-01249-7.dvi; http://www.ams.org/mcom/2000-69-231/S0025-5718-00-01249-7/S0025-5718-00-01249-7.pdf; http://www.ams.org/mcom/2000-69-231/S0025-5718-00-01249-7/S0025-5718-00-01249-7.ps; http://www.ams.org/mcom/2000-69-231/S0025-5718-00-01249-7/S0025-5718-00-01249-7.tex.

Walter:2001:PBM

[Wal01] Colin D. Walter. Precise bounds for Montgomery modular multiplication and some potentially insecure RSA moduli. *Lecture Notes in Computer Science*, 2271: 30–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710030.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710030.pdf.

Walter:2003:STM

[Wal03] Colin D. Walter. Seeing through MIST given a small fraction of an RSA private key. In Joye [Joy03b], pages 391–402. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Wallich:2004:EEI

[Wal04] P. Wallich. Electrical engineering's identity crisis — when does a vast and vital profession become unrecognizably diffuse? *IEEE Spectrum*, 41 (11):66–73, November 2004. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Wallich:2009:SGP

[Wal09] P. Wallich. The supercomputer goes personal. *IEEE Spectrum*, 46(4):64, April 2009. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Wang:2004:AWA

[Wan04a] Shiuh-Jeng Wang. Anonymous wireless authentication on a portable cellular mobile system. *IEEE Transactions on Computers*, 53(10):1317–1329, October 2004. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1327581.

Wang:2004:TVS

[Wan04b] Shiuh-Jeng Wang. Threshold verification scheme to a valid-signature using identity only on specialized approval. *Applied Mathematics and Computation*, 152 (2):373–383, May 5, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Wang:2005:SCR

[Wan05] Shiuh-Jeng Wang. Steganography of capacity required using modulo operator for embedding secret image. *Applied Mathematics and Computation*, 164(1):99–116, May 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Wardlaw:2000:RPK

[War00] William P. Wardlaw. The RSA public key cryptosystem. In *Coding theory and cryptography (Annapolis, MD, 1998)*, pages 101–123. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000.

Washington:2008:BRB

[Was08a] Lawrence C. Washington. Book review: *Handbook* *of Elliptic and Hyperelliptic Curve Cryptography*, by H. Cohen and G. Frey, Chapman & Hall/CRC, 2006, 1-58488-518-1. *ACM SIGACT News*, 39(1):19–22, March 2008. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL `http://doi.acm.org/10.1145/1360443.1360448`. See [CFA+06].

Washington:2008:ECN

[Was08b] Lawrence C. Washington. *Elliptic curves: number theory and cryptography*. Discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, second edition, 2008. ISBN 1-4200-7146-7 (hardcover). xviii + 513 pp. LCCN QA567.2.E44 W37 2008.

Wayman:2001:FBA

[Way01] J. L. Wayman. Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics (IJIG)*, 1(1): 93–??, January 2001. CODEN ???? ISSN 0219-4678.

Wayman:2002:BAT

[Way02a] James L. Wayman. Biometric authentication technologies: Hype meets the test results, 2002. URL `http://www.usenix.org/publications/library/proceedings/sec02/tech.html`. Unpublished.

Wayner:2002:DCI

[Way02b] Peter Wayner. *Disappearing cryptography: information hiding: steganography & watermarking*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, second edition, 2002. ISBN 1-55860-769-2. xvii + 413 pp. LCCN TK5105.59 .W39 2002. US$44.95.

Wayner:2009:DCI

[Way09] Peter Wayner. *Disappearing cryptography: information hiding: steganography and watermarking*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, third edition, 2009. ISBN 0-12-374479-2, 0-08-092270-8 (e-book). xv + 439 pp. LCCN TK5105.59 .W39 2009. URL `http://www.sciencedirect.com/science/book/9780123744791`.

Weiss:2000:CAC

[WB00] Richard Weiss and Nathan Binkert. A comparison of AES candidates on the Alpha 21264. In NIST [NIS00], pages 75–81. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf`;

http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Wu:2002:CSCa

[WB02] Hongjun Wu and Feng Bao. Cryptanalysis of stream cipher COS$^{(2,128)}$ Mode I. *Lecture Notes in Computer Science*, 2384: 154–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840154.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840154.pdf.

Wu:2001:CDS

[WBD01] Hongjun Wu, Feng Bao, and Robert H. Deng. Cryptanalysis of a digital signature scheme on ID-based key-sharing infrastructures. *Lecture Notes in Computer Science*, 1992: 173–179, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920173.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920173.pdf.

Weis:2001:SYH

[WBL01] Rüdiger Weis, Bastiaan Bakker, and Stefan Lucks. Security on your hand: Secure filesystems with a "non-cryptographic" JAVA-ring. *Lecture Notes in Computer Science*, 2041: 151–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2041/20410151.htm; http://link.springer-ny.com/link/service/series/0558/papers/2041/20410151.pdf.

Weeks:2000:HPS

[WBRF00] Bryan Weeks, Mark Bean, Tom Rozylowicz, and Chris Ficke. Hardware performance simulations of round 2 Advanced Encryption Standard algorithms. In NIST [NIS00], pages 286–304. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/

conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Wong:2001:EMA

[WC01a] Duncan S. Wong and Agnes H. Chan. Efficient and mutually authenticated key exchange for low power computing devices. *Lecture Notes in Computer Science*, 2248:272–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480272.htm; http://link.springer-ny.com/link/service/series/0558/papers/2248/22480272.pdf.

Wu:2001:CKA

[WC01b] T.-C. Wu and C.-C. Chang. Cryptographic key assignment scheme for hierarchical access control. *International Journal of Computer Systems Science and Engineering*, 16(1):??, January 2001. CODEN CSSEEI. ISSN 0267-6192.

Wu:2003:HDW

[WC03a] Hsien-Chu Wu and Chin-Chen Chang. Hiding digital watermarks using fractal compression technique. *Fundamenta Informaticae*, 58(2):189–202, April 2003. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Wu:2003:UFR

[WC03b] Shyi-Tsong Wu and Bin-Chang Chieu. A user friendly remote authentication scheme with smart cards. *Computers & Security*, 22(6):547–550, September 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803006163.

Wu:2004:EIW

[WC04] Hsien-Chu Wu and Chin-Chen Chang. Embedding invisible watermarks into digital images based on side-match vector quantization. *Fundamenta Informaticae*, 63(1):89–106, January 2004. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Wu:2005:NDI

[WC05] Hsien-Chu Wu and Chin-Chen Chang. A novel digital image watermarking scheme based on the vector quantization technique. *Computers & Security*, 24(6):460–471, September 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https:/

/www.sciencedirect.com/science/article/pii/S0167404805000672.

Wang:2005:TAP

[WCJ05] Xinyuan Wang, Shiping Chen, and Sushil Jajodia. Tracking anonymous peer-to-peer VoIP calls on the Internet. In Meadows and Syverson [MS05b], pages 81–91. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Wang:2009:NWA

[WCJ09] Chung-Chuan Wang, Chin-Chen Chang, and Jinn-Ke Jan. Novel watermarking authentication schemes for binary images based on dual-pair block pixel patterns. *Fundamenta Informaticae*, 90(1–2):125–155, January 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Wang:2005:SDR

[WCZ05] Kun Wang, Zhen Cai, and Lihua Zhou. Study on disaster recovery planning model. In Han et al. [HYZ05b], pages 151–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Westerlund:2001:HWK

[WD01a] Assar Westerlund and Johan Danielsson. Heimdal and Windows 2000 Kerberos — how to get them to play together. In USENIX [USE01b], page ?? ISBN 1-880446-10-3. LCCN QA76.8.U65 U84 2001. URL http://www.usenix.org/publications/library/proceedings/usenix01/freenix01/westerlund.html.

Williams:2001:ICA

[WD01b] Jeannette Williams and Yolande Dickerson. *The Invisible Cryptologists: African-Americans, WWII to 1956*. Center for Cryptologic History, National Security Agency, Fort Meade, MD, USA, 2001. viii + 43 pp. URL https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/wwii/assets/files/invisible_cryptologists.pdf.

Weir:2009:UPS

[WDCJ09] Catherine S. Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1–2):47–62, February/March 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808000941.

Wang:2009:SST

[WDLN09] Ronghua Wang, Wenliang

Du, Xiaogang Liu, and Peng Ning. ShortPK: a short-term public key scheme for broadcast authentication in sensor networks. *ACM Transactions on Sensor Networks*, 6(1):9:1–9:??, December 2009. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Weaver:2006:BA

[Wea06] Alfred C. Weaver. Biometric authentication. *Computer*, 39(2):96–97, February 2006. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Weber:2002:ECH

[Web02] Arnd Weber. Enabling crypto: how radical innovations occur. *Communications of the Association for Computing Machinery*, 45(4):103–107, April 2002. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Webb:2008:IZN

[Web08] Charles F. Webb. IBM z10: The next-generation mainframe microprocessor. *IEEE Micro*, 28(2):19–29, March/April 2008. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Wehde:2000:IME

[Weh00] Ed Wehde. IBM, Microsoft in encryption effort. *Network Security*, 2000(2):5, February 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800876540.

Weierud:2000:SFB

[Wei00] Frode Weierud. Sturgeon, the FISH BP never really caught. In Joyner [Joy00], page ?? ISBN 3-540-66336-3 (softcover), 3-642-59663-0 (e-book). LCCN QA268 .C67 1999. UK£44.50. URL http://frode.home.cern.ch/frode/pubs/cryptoday.pdf. Proceedings of the Conference on Coding Theory, Cryptography and Number Theory held at the U.S. Naval Academy during October 25–26, 1998.

Weiss:2004:JCE

[Wei04] Jason Weiss. *Java Cryptography Extensions: Practical Guide for Programmers*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 2004. ISBN 0-12-742751-1. xv + 158 pp. LCCN QA76.73.J38 W445 2004. US$21.95.

Weierud:2005:BSF

[Wei05] Frode Weierud. BP's sturgeon, the FISH that laid no eggs. In Copeland [Cop05], page ?? ISBN 0-19-284055-X. LCCN D810.C88 C66 2006.

Weierud:2005:BPS

[Wei06] Frode Weierud. Bletchley Park's Sturgeon, the fish that laid no eggs. *Rutherford Journal*, 1(??): ??, ???? 2005–2006. CODEN ???? ISSN 1177-1380. URL http://rutherfordjournal.org/article010106.html.

Welschenbach:2005:CCC

[Wel05] Michael Welschenbach. *Cryptography in C and C++*. Apress, Berkeley, CA, USA, second edition, 2005. ISBN 1-59059-502-5. xxv + 478 pp. LCCN QA76.9.A25 W4313 2005. URL http://www.loc.gov/catdir/enhancements/fy0663/2005002553-d.html; http://www.loc.gov/catdir/toc/ecip057/2005002553.html.

Weng:2003:CHC

[Wen03] Annegret Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72(241):435–458, January 2003. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journal-getitem?pii=S0025-5718-02-01422-9; http://www.ams.org/mcom/2003-72-241/S0025-5718-02-01422-9/S0025-5718-02-01422-9.dvi; http://www.ams.org/mcom/2003-72-241/S0025-5718-02-01422-9/S0025-5718-02-01422-9.pdf; http://www.ams.org/mcom/2003-72-241/S0025-5718-02-01422-9/S0025-5718-02-01422-9.ps; http://www.ams.org/mcom/2003-72-241/S0025-5718-02-01422-9/S0025-5718-02-01422-9.tex.

Wernsdorf:2002:RFR

[Wer02] Ralph Wernsdorf. The round functions of RIJNDAEL generate the alternating group. *Lecture Notes in Computer Science*, 2365:143–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650143.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650143.pdf.

Westfeld:2001:FSA

[Wes01] Andreas Westfeld. F5 — A steganographic algorithm. *Lecture Notes in Computer Science*, 2137: 289–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370289.htm;

http://link.springer-ny.com/link/service/series/0558/papers/2137/21370289.pdf.

Wu:2002:LCN

[WF02] Wenling Wu and Dengguo Feng. Linear cryptanalysis of NUSH block cipher. *Sci. China Ser. F*, 45(1):59–67, 2002. ISSN 1009-2757.

Wang:2004:CHF

[WFLY04] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. Cryptology ePrint Archive, Report 2004/199, 2004. URL http://eprint.iacr.org/2004/199.pdf; http://www.tcs.hut.fi/~mjos/md5/.

Wang:2002:CSE

[WG02] Xiang Sheng Wang and Juan Ren Gan. A chaotic sequence encryption method. *Chinese Journal of Computers = Chi suan chi hsueh pao*, 25(4):351–356, 2002. CODEN JIXUDT. ISSN 0254-4164.

Wang:2005:RST

[WG05] Lijun Wang and Chao Gao. Rough set theory's application on intrusion detection based on system calls. In Han et al. [HYZ05b], pages 83–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Wong:2000:SGC

[WGL00] Chung Kei Wong, Mohamed Gouda, and Simon S. Lam. Secure group communications using key graphs. *IEEE/ACM Transactions on Networking*, 8(1):16–30, February 2000. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL http://www.acm.org/pubs/citations/journals/ton/2000-8-1/p16-wong/.

Wu:2002:CAE

[WH02a] Tzong-Sun Wu and Chien-Lung Hsu. Convertible authenticated encryption scheme. *The Journal of Systems and Software*, 62(3):205–209, June 15, 2002. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Wu:2002:IBM

[WH02b] Tzong-Sun Wu and Chien-Lung Hsu. ID-based multisignatures with distinguished signing authorities for sequential and broadcasting architectures. *Applied Mathematics and Computation*, 131(2–3):349–356, September 25, 2002. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Wu:2003:TSS

[WH03] Tzong-Sun Wu and Chien-Lung Hsu. Threshold signature scheme using self-certified public keys. *The Journal of Systems and Software*, 67(2):89–97, August 15, 2003. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Wang:2009:NWM

[WH09] Yu-Ping Wang and Shi-Min Hu. A new watermarking method for 3D models based on integral invariants. *IEEE Transactions on Visualization and Computer Graphics*, 15(2):285–294, March/April 2009. CODEN ITVGEA. ISSN 1077-2626 (print), 1941-0506 (electronic), 2160-9306.

Wen:2005:URE

[WHH05] Hsiang-An Wen, Sheng-Yu Hwang, and Tzonelih Hwang. On the unlinkability of randomization-enhanced Chaum's blind signature scheme. *Applied Mathematics and Computation*, 164(3):799–803, May 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Wu:2008:RPG

[WHHT08] Tzong-Chen Wu, Thsia-Tzu Huang, Chien-Lung Hsu, and Kuo-Yu Tsai. Recursive protocol for group-oriented authentication with key distribution. *The Journal of Systems and Software*, 81(7):1227–1239, July 2008. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Watanabe:2001:EAP

[WHI01] Yuji Watanabe, Goichiro Hanaoka, and Hideki Imai. Efficient asymmetric public-key traitor tracing without trusted agents. *Lecture Notes in Computer Science*, 2020:392–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200392.htm; http://link.springer-ny.com/link/service/series/0558/papers/2020/20200392.pdf`.

White:2009:EOD

[Whi09] Tobin White. Encrypted objects and decryption processes: problem-solving with functions in a learning environment based on cryptography. *Educational Studies in Mathematics*, 72(1):17–37, September 2009. CODEN EDSMAN. ISSN 0013-1954 (print), 1573-0816 (electronic). URL `http://link.springer.com/content/pdf/`

10.1007/s10649-008-9180-y.pdf.

Wu:2005:SSP

[WHL05] Hsien-Chu Wu, Min-Shiang Hwang, and Chia-Hsin Liu. A secure strong-password authentication protocol. *Fundamenta Informaticae*, 68(4):399–406, June 2005. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Wu:2003:IMT

[WHLH03] Tzong-Sun Wu, Chien-Lung Hsu, Han-Yu Lin, and Po-Sheng Huang. Improvement of the Miyazaki–Takaragi threshold digital signature scheme. *Information Processing Letters*, 88(4):183–186, November 30, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Wang:2005:EAS

[WHLH05] Fei Wang, Yupu Hu, Ying Liu, and Zhanpeng Hu. An efficient algorithm for software generation of the generalized self-shrinking sequence. In Han et al. [HYZ05b], pages 163–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Whyte:2005:TFC

[Why05] William Whyte. Towards faster cryptosystems, I. In Garrett and Lieman [GL05], pages 113–137. ISBN 0-8218-3365-0. LCCN QA76.9.A25 P82 2005. URL http://www.loc.gov/catdir/toc/fy0612/2005048178.html.

Wiener:2000:AAH

[Wie00] Michael J. Wiener. Algorithm alley: High-speed cryptography with the RSA algorithm. *Dr. Dobb's Journal of Software Tools*, 25(2):123–126, February 2000. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ftp/2000/2000_02/aa220.txt.

Williams:1999:QCQ

[Wil99] Colin P. Williams, editor. *Quantum computing and quantum communications: First NASA International Conference, QCQS [i.e., QCQC] '98, Palm Springs, California, USA, February 17–20, 1998: selected papers*, volume 1509 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-65514-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.889 .Q37 1998.

Wilcox:2001:SEH

[Wil01a] Jennifer E. Wilcox. Solving the Enigma: history of the cryptanalytic bombe. Report, National Security Agency/Central Security Service. Center for Cryptologic History, Fort George G. Meade, MD, USA, January 2001. 52 pp.

Wilson:2001:PBA

[Wil01b] Gregory V. Wilson. Programmer's bookshelf: Alien worlds. *Dr. Dobb's Journal of Software Tools*, 26(12): 122, 124, December 2001. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/`.

Williams:2006:C

[Wil06] Conrad Williams. *The cryptanalyst*. Leaf, Abercynon, UK, 2006. ISBN 1-905599-23-4. 32 pp. LCCN ????

Winterbotham:2000:USI

[Win00] F. W. (Frederick William) Winterbotham. *The Ultra secret: the inside story of Operation Ultra, Bletchley Park and Enigma*. Orion, London, UK, 2000. ISBN 0-7528-3751-6. xv + 199 pp. LCCN ????

Wincelberg:2001:JQH

[Win01] David Wincelberg. Java Q&A: How do you use the `javax.crypto` package? *Dr. Dobb's Journal of Software Tools*, 26(4): 139–140, April 2001. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ftp/2001/2001_04/jqa0401.txt`; `http://www.ddj.com/ftp/2001/2001_04/jqa0401.zip`.

Windley:2005:DI

[Win05a] Phillip J. Windley. *Digital identity*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, 2005. ISBN 0-596-00878-3. xviii + 234 pp. LCCN TK5105.59 .W45 2005.

Winkel:2005:GEC

[Win05b] Brian J. Winkel, editor. *The German Enigma cipher machine*. Artech House computer security series. Artech House Inc., Norwood, MA, USA, 2005. ISBN 1-58053-996-3. ???? pp. LCCN D810.C88 G47 2005.

Winkler:2005:SAU

[Win05c] Ira Winkler. *Spies among us: how to stop the spies, terrorists, hackers, and criminals you don't even know you encounter every day*. John Wiley and Sons, Inc., New York, NY, USA, 2005. ISBN 0-7645-8468-5 (cloth). xix + 326 pp. LCCN UB250 .W55 2005. URL `http://www.loc.gov/catdir/toc/ecip054/2004028735.html`;

http://www.wiley.com/WileyCDA/WileyTitle/productCd-0764584685.html.

Withers:2001:IWU

[Wit01] Alex Withers. Integrating Windows 2000 and UNIX using Kerberos. *Sys Admin: The Journal for UNIX Systems Administrators*, 10 (12):39, 41–42, 44, December 2001. CODEN SYADE7. ISSN 1061-2688.

Wang:2007:VBW

[WJP07] Feng-Hsing Wang, Lakhmi C. Jain, and Jeng-Shyang Pan. VQ-based watermarking scheme with genetic codebook partition. *Journal of Network and Computer Applications*, 30(1):4–23, January 2007. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480450500038X.

Welschenbach:2001:CCC

[WK01] Michael Welschenbach and David Kramer. *Cryptography in C and C++*. Apress, Berkeley, CA, USA, second edition, 2001. ISBN 1-893115-95-X. xix + 432 pp. LCCN QA76.73.C153 W457 2001. UK£35.50.

Wang:2005:ECSb

[WK05] Chih-Hung Wang and Yan-Sheng Kuo. An efficient contract signing protocol using the aggregate signature scheme to protect signers' privacy and promote reliability. *Operating Systems Review*, 39(4):66–79, October 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Won:2006:ISC

[WK06] Dongho Won and Seungjoo Kim, editors. *Information security and cryptology — ICISC 2005: 8th international conference, Seoul, Korea, December 1–2, 2005, revised selected papers*, volume 3935 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-33354-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3935.

Weigold:2008:RCA

[WKB08] Thomas Weigold, Thorsten Kramp, and Michael Baentsch. Remote client authentication. *IEEE Security & Privacy*, 6(4):36–43, July/August 2008. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Walter:2003:CHE

[WKP03] Colin D. Walter, Çetin K. Koç, and Christof Paar, editors. *Cryptographic Hardware and Embedded Systems—CHES 2003: 5th International Workshop, Cologne, Germany, September 8–10, 2003: Proceedings*, volume 2779 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2779; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13240.

Wang:2002:AAB

[WL02] Lusheng Wang and Zimao Li. An approximation algorithm for a bottleneck k-Steiner tree problem in the Euclidean plane. *Information Processing Letters*, 81(3):151–156, February 14, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.com/gej-ng/10/23/20/85/34/32/abstract.html.

Wedde:2004:MAA

[WL04a] Horst F. Wedde and Mario Lischka. Modular authorization and administration. *ACM Transactions on Information and System Security*, 7(3):363–391, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wu:2004:RKA

[WL04b] Tzong-Sun Wu and Han-Yu Lin. Robust key authentication scheme resistant to public key substitution attacks. *Applied Mathematics and Computation*, 157(3):825–833, October 15, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Wang:2005:CHY

[WL05] Shyh-Yih Wang and Chi-Sung Laih. Cryptanalysis of Hwang–Yang scheme for controlling access in large partially ordered hierarchies. *The Journal of Systems and Software*, 75(1–2):189–192, February 15, 2005. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Wang:2007:NCD

[WL07a] Zhenghong Wang and Ruby B. Lee. New cache designs for thwarting software cache-based side channel attacks.

ACM SIGARCH Computer Architecture News, 35(2): 494–505, May 2007. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Williams:2007:FTA

[WL07b] D. Williams and H. Lutfiyya. Fault-tolerant authentication services. *International Journal of Computer Applications*, 29(2): 107–114, 2007. CODEN IJCAFW. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2007.11441838`.

Wen:2006:PSA

[WLH06] Hsiang-An Wen, Chun-Li Lin, and Tzonelih Hwang. Provably secure authenticated key exchange protocols for low power computing clients. *Computers & Security*, 25(2):106–113, March 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404805001732`.

Wen:2005:TRB

[WLHH05] Hsiang-An Wen, Kuo-Chang Lee, Sheng-Yu Hwang, and Tzonelih Hwang. On the traceability on RSA-based partially signature with low computation. *Applied Mathematics and Computation*, 162(1):421–425, March 4, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Wang:2009:DSM

[WLLL09] J. Wang, J. Lü, S. Lian, and G. Liu. On the design of secure multimedia authentication. *J.UCS: Journal of Universal Computer Science*, 15(2):426–??, ???? 2009. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_15_2/on_the_design_of`.

Wang:2003:CET

[WLT03] Bin Wang, Jian-Hua Li, and Zhi-Peng Tong. Cryptanalysis of an enhanced timestamp-based password authentication scheme. *Computers & Security*, 22(7): 643–645, October 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404803007132`.

Wang:2005:SAI

[WLT05a] Yingjie Wang, J. H. Li, and L. Tie. Security analysis and improvement of a user-friendly remote authentication protocol. *Applied Mathematics and Computation*, 168(1):47–50, September 1, 2005. CODEN AMHCBQ.

ISSN 0096-3003 (print), 1873-5649 (electronic).

Wu:2005:IAW

[WLT05b] Qiong Wu, Guohui Li, and Dan Tu. An image authentication watermarking with self-localization and recovery. In Han et al. [HYZ05b], pages 960–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Wong:2004:RCK

[WLW04] W. K. Wong, L. P. Lee, and K. W. Wong. Reply to the comment "Keystream cryptanalysis of a chaotic cryptographic method". *Computer Physics Communications*, 156(2):208, January 1, 2004. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465503004338. See [kWpLwW01, ÁMRP04].

Wang:2005:TSP

[WLZZ05] Yu Wang, Yichao Li, Xiaosong Zhang, and Jiazhi Zeng. Tracing single-packet attacks to their sources. In Han et al. [HYZ05b], pages 118–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Wu:2008:RWM

[WMDR08] Xiaomao Wu, Lizhuang Ma, Zhuoqun Dong, and Lionel Revéret. Robust watermarking motion data with DL-STDM. *Computers and Graphics*, 32(3):320–329, June 2008. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0097849308000447.

Watters:2008:VDL

[WMS08] Paul Watters, Frances Martin, and H. Steffen Stripf. Visual detection of LSB-encoded natural image steganography. *ACM Transactions on Applied Perception*, 5(1):5:1–5:??, January 2008. CODEN ???? ISSN 1544-3558 (print), 1544-3965 (electronic).

Wheeler:1995:TTE

[WN95] D. J. Wheeler and R. M. Needham. TEA, a tiny encryption algorithm. *Lecture Notes in Computer Science*, 1008:363–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Watanabe:2002:CCD

[WN02] Yuji Watanabe and Masayuki Numao. Conditional cryptographic delegation for P2P data sharing. *Lecture Notes in Computer Science*,

2433:309–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330309.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330309.pdf.

Wang:2008:NAD

[WNQ08] Xiang-Yang Wang, Pan-Pan Niu, and Wei Qi. A new adaptive digital audio watermarking based on support vector machine. *Journal of Network and Computer Applications*, 31(4):735–749, November 2008. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804507000525.

Wang:2009:RDA

[WNY09] Xiang-Yang Wang, Pan-Pan Niu, and Hong-Ying Yang. A robust, digital-audio watermarking method. *IEEE MultiMedia*, 16(3):60–69, July/September 2009. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Wolkerstorfer:2001:AIA

[WOL01] Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger. An ASIC implementation of the AES SBoxes. *Lecture Notes in Computer Science*, 2271:67–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710067.htm; http://link.springer-ny.com/link/service/series/0558/papers/2271/22710067.pdf.

Wolfe:2003:EE

[Wol03] Hank Wolfe. Encountering encryption. *Computers & Security*, 22(5):388–391, July 2003. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404803005042.

Wollinger:2004:SHI

[Wol04] Thomas Wollinger. *Software and hardware implementation of hyperelliptic curve cryptosystems*, volume 3 of *IT-Security*. Europäischer Universitätsverlag, Bochum, Germany, 2004. ISBN 3-86515-025-X. 177 pp. LCCN ???? EUR 24.90. URL http://verlag.rub.de/g9783865150257.html.

Won:2001:ISC

[Won01] Dongho Won, editor. *Information security and cryptology: ICISC 2000, Third*

International Conference, Seoul, Korea, December 8–9, 2000: Proceedings, volume 2015 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-41782-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I32 2000; QA267.A1 L43 no.2015. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2015.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2015`.

Wool:2000:KME

[Woo00] Avishai Wool. Key management for encrypted broadcast. *ACM Transactions on Information and System Security*, 3(2):107–134, May 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wood:2005:IIM

[Woo05] Peter Wood. Implementing identity management security — an ethical hacker's view. *Network Security*, 2005(9):12–15, September 2005. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485805702828`.

Wang:2003:SGP

[WP03] Huaxiong Wang and Josef Pieprzyk. Shared generation of pseudo-random functions with cumulative maps. In Joye [Joy03b], pages 281–294. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612`.

Wollinger:2005:CVH

[WPP05] T. Wollinger, J. Pelzl, and C. Paar. Cantor versus Harley: optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems. *IEEE Transactions on Computers*, 54(7):861–872, July 2005. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1432669`.

Weimerskirch:2001:ECC

[WPS01] André Weimerskirch, Christof Paar, and Sheueling Chang Shantz. Elliptic curve cryptography on a palm OS device. *Lecture Notes in Computer Science*, 2119: 502–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190502.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190502.pdf.

Wang:2001:TUR

[WQWZ01] Guilin Wang, Sihan Qing, Mingsheng Wang, and Zhanfei Zhou. Threshold undeniable RSA signature scheme. *Lecture Notes in Computer Science*, 2229:221–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290221.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290221.pdf.

Wright:2000:IQC

[Wri00] Marie A. Wright. The impact of quantum computing on cryptography. *Network Security*, 2000(9):13–15, September 1, 2000. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800090279.

Wright:2001:AES

[Wri01] Marie A. Wright. The Advanced Encryption Standard. *Network Security*, 2001(10):11–13, October 31, 2001. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485801010182.

Wright:2003:FCI

[Wri03] Rebecca N. Wright, editor. *Financial cryptography: 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27–30, 2003: revised papers*, volume 2742 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-40663-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 2003. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2742; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b11831.

Wrixon:2005:CCO

[Wri05] Fred B. Wrixon. *Codes, Ciphers and Other Cryptic* *and Clandestine Communication: Making and Breaking Secret Messages from Hieroglyphs to the Internet.* Black Dog & Leventhal Publishers, New York, NY, USA, 2005. ISBN 1-57912-485-2. 704 pp. LCCN Z103.3 .W75 1998.

Wang:2002:IPD

[WRW02] Xinyuan Wang, Douglas S. Reeves, and S. Felix Wu. Inter-packet delay based correlation for tracing encrypted connections through stepping stones. *Lecture Notes in Computer Science*, 2502:244–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2502/25020244.htm`; `http://link.springer.de/link/service/series/0558/papers/2502/25020244.pdf`.

Wright:2002:EPS

[WS02] R. N. Wright and S. Spalding. Experimental performance of shared RSA modulus generation. *Algorithmica*, 33(1):89–103, January 2002. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=33&issue=1&spage=89`. Experimental algorithms.

Whiting:2003:MPH

[WS03] Douglas L. Whiting and Michael J. Sabin. Montgomery prime hashing for message authentication. In Joye [Joy03b], pages 50–67. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612`.

Walter:2005:DDP

[WS05] Colin Walter and David Samyde. Data dependent power use in multipliers. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL `http://arith17.polito.it/final/paper-126.pdf`.

Weimerskirch:2002:DLW

[WT02] André Weimerskirch and Gilles Thonet. A distributed light-weight authentication model for ad-hoc networks. *Lecture Notes in Computer Science*, 2288:341–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880341.htm`;

http://link.springer-ny.com/link/service/series/0558/papers/2288/22880341.pdf.

Wu:2001:DSM

[Wu01] T.-C. Wu. Digital signature/multisignature schemes giving public key verification and message recovery simultaneously. *International Journal of Computer Systems Science and Engineering*, 16(6):??, November 2001. CODEN CSSEEI. ISSN 0267-6192.

Wu:2002:CSCb

[Wu02] Hongjun Wu. Cryptanalysis of stream cipher Alpha1. *Lecture Notes in Computer Science*, 2384: 169–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840169.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840169.pdf.

Wuensche:2009:CAE

[Wue09] Andrew Wuensche. Cellular Automata Encryption: the reverse algorithm, Z-parameter and chain-rules. *Parallel Processing Letters*, 19(2):283–297, June 2009. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Wu:2000:PKC

[WV00] Chuan-Kun Wu and Vijay Varadharajan. Public key cryptosystems based on Boolean permutations and their applications. *International Journal of Computer Mathematics*, 74(2): 167–184, 2000. CODEN IJCMAT. ISSN 0020-7160.

Wu:2001:FED

[WV01] Chuan-Kun Wu and Vijay Varadharajan. Fair exchange of digital signatures with offline trusted third party. *Lecture Notes in Computer Science*, 2229: 466–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290466.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290466.pdf.

Woodruff:2002:CUC

[WvD02] David P. Woodruff and Marten van Dijk. Cryptography in an unbounded computational model. *Lecture Notes in Computer Science*, 2332:149–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320149.htm;

http://link.springer-ny.com/link/service/series/0558/papers/2332/23320149.pdf.

Weaver:2000:CAC

[WW00] Nicholas Weaver and John Wawrzynek. A comparison of the AES candidates amenability to FPGA implementation. In NIST [NIS00], pages 28–39. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Wang:2004:CWS

[WW04] Huaiqing Wang and Shuozhong Wang. Cyber warfare: steganography vs. steganalysis. *Communications of the Association for Computing Machinery*, 47(10):76–82, October 2004. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Wolf:2005:NML

[WW05] Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. In Shoup [Sho05a], pages 467–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Wang:2006:SPS

[WW06] Chung-Ming Wang and Peng-Cheng Wang. Steganography on point-sampled geometry. *Computers and Graphics*, 30(2):244–254, April 2006. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.sciencedirect.com/science/article/pii/S009784930600032X.

Wang:2008:DCP

[WW08] Xing-Yuan Wang and Xiao-Juan Wang. Design of chaotic pseudo-random bit generator and its applications in stream-cipher cryptography. *International Journal of Modern Physics C [Physics and Computers]*, 19(5):813–820, May 2008. CODEN IJM-

PEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL http://www.worldscinet.com/ijmpc/19/1905/S0129183108012479.html.

Wu:2001:CFF

[WWA01] Lisa Wu, Chris Weaver, and Todd Austin. CryptoManiac: a fast flexible architecture for secure communication. *ACM SIGARCH Computer Architecture News*, 29(2):110–119, May 2001. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Worley:2000:AFP

[WWCW00] John Worley, Bill Worley, Tom Christian, and Christopher Worley. AES finalists on PA-RISC and IA-64: Implementations & performance. In NIST [NIS00], pages 57–74. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Wollinger:2000:HWH

[WWGP00] Thomas J. Wollinger, Min Wang, Jorge Guajardo, and Christof Paar. How well are high-end DSPs suited for the AES algorithms? AES algorithms on the TMS320C6x DSP. In NIST [NIS00], pages 94–105. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Wincelberg:2002:LIE

[WWL+02] David Wincelberg, Sy Wong, Dan Leach, Paul Keister, and Robert Masta. Letters: Inside eBook security; numerical weather forecasting; FrontPage EULA; priority queues; audio watermarking versus compression. *Dr. Dobb's Journal of Software Tools*, 27(3):10, March 2002. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Wang:2008:HQS

[WWTH08] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, and Min-Shiang Hwang. A high quality steganographic method with pixel-value differencing and modulus function. *The Journal of Systems and Software*, 81 (1):150–158, January 2008. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Wang:2002:WEM

[WY02] Shiuh-Jeng Wang and Kai-Sheng Yang. Watermark embedding mechanism using modulus-based for intellectual property protection on image data. *Lecture Notes in Computer Science*, 2455:333–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2455/24550333.htm; http://link.springer-ny.com/link/service/series/0558/papers/2455/24550333.pdf.

Wu:2005:CTR

[WY05] Lin-Chuan Wu and Yi-Shiung Yeh. Comment on traceability on RSA-based partially signature with low computation. *Applied Mathematics and Computation*, 170(2):1344–1348, November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Wyant:2002:APK

[Wya02] Jeremy Wyant. Applicability of public key cryptosystems to digital rights management applications. *Lecture Notes in Computer Science*, 2339:75–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2339/23390075.htm; http://link.springer-ny.com/link/service/series/0558/papers/2339/23390075.pdf.

Wyler:2005:ANS

[Wyl05] Neil R. Wyler. *Aggressive network self-defense*. Syngress Publishing, Inc., Rockland, MA, USA, 2005. ISBN 1-931836-20-5. xxx + 383 pp. LCCN QA76.9.A25 A38 2005; QA76.9.A25 A447 2005. URL http://site.ebrary.com/lib/ucsc/Doc?id=10075669.

Wang:2005:CSA

[WYY05a] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Collision search attacks on SHA1. Technical report, Shandong University, Shandong, China, 2005. URL http://

theory.csail.mit.edu/~yiqun/shanote.pdf.

Wang:2005:FCFa

[WYY05b] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. Technical report, Shandong University, Shandong, China, June 22, 2005. URL http://cryptome.org/wang_sha1_v2.zip.

Wang:2005:FCFb

[WYY05c] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Wang:2005:ECSa

[WYY05d] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. Efficient collision search attacks on SHA-0. In Shoup [Sho05a], pages 1–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Winslett:2005:PLD

[WZB05] Marianne Winslett, Charles C. Zhang, and Piero A. Bonatti. PeerAccess: a logic for distributed authorization. In Meadows and Syverson [MS05b], pages 168–179. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Wang:2005:DIC

[WZW05] Xuebing Wang, Linhua Zhang, and Yong Wu. Design and implementation of a chaos-based public key encryption scheme. In Han et al. [HYZ05b], pages 79–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Xu:2001:EIE

[XB01] Sheng-Bo Xu and Lejla Batina. Efficient implementation of elliptic curve cryptosystems on an ARM7 with hardware accelerator. *Lecture Notes in Computer Science*, 2200: 266–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/

link/service/series/0558/bibs/2200/22000266.htm; http://link.springer-ny.com/link/service/series/0558/papers/2200/22000266.pdf.

Xu:2005:ETR

[XC05] Qiu-Liang Xu and Tzer-Shyong Chen. An efficient threshold RSA digital signature scheme. *Applied Mathematics and Computation*, 166(1):25–34, July 6, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Xu:2001:CPW

[XFZ01] Changsheng Xu, David Dagan Feng, and Yongwei Zhu. Copyright protection for WAV-table synthesis audio using digital watermarking. *Lecture Notes in Computer Science*, 2195:772–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2195/21950772.htm; http://link.springer-ny.com/link/service/series/0558/papers/2195/21950772.pdf.

Xiao:2003:HPC

[XH03] Lu Xiao and Howard M. Heys. Hardware performance characterization of block cipher structures. In Joye [Joy03b], pages 176–192. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Xiao:2005:SPA

[XH05] Lu Xiao and Howard M. Heys. A simple power analysis attack against the key schedule of the Camellia block cipher. *Information Processing Letters*, 95(3):409–412, August 16, 2005. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Xenakis:2006:GCO

[XLMS06] Christos Xenakis, Nikolaos Laoutaris, Lazaros Merakos, and Ioannis Stavrakakis. A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms. *Computer Networks (Amsterdam, Netherlands: 1999)*, 50(17):3225–3241, December 5, 2006. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Xu:2007:CAD

[XMST07] Changsheng Xu, Namunu C.

Maddage, Xi Shao, and Qi Tian. Content-adaptive digital music watermarking based on music structure analysis. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 3(1):??, February 2007. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Xu:2005:ADR

[XNK+05] Jun Xu, Peng Ning, Chongkyung Kil, Yan Zhai, and Chris Bookholt. Automatic diagnosis and response to memory corruption vulnerabilities. In Meadows and Syverson [MS05b], pages 223–234. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Xie:2007:ISP

[XQ07] Tao Xie and Xiao Qin. Improving security for periodic tasks in embedded systems through scheduling. *ACM Transactions on Embedded Computing Systems*, 6(3): 20:1–20:??, July 2007. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Xu:2003:TEP

[XS03] Shouhuai Xu and Ravi Sandhu. Two efficient and provably secure schemes for server-assisted threshold signatures. In Joye [Joy03b], pages 355–372. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612`.

Xin:2010:IEB

[XSWC10] Hong Xin, Zhu Shujing, Chen Weibin, and Jian Chongjun. An image encryption base on non-linear pseudo-random number generator. In *2010 International Conference on Computer Application and System Modeling (ICCASM)*, volume 9, pages V9–238–V9–241. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5623043`.

Xiang:2008:CPA

[XwWL08] Tao Xiang, Kwok wo Wong, and Xiaofeng Liao. Cryptanalysis of a password authentication scheme over insecure networks. *Journal of Computer and System Sciences*, 74(5):657–661, August 2008. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000007000657.

Xie:2004:CTA

[XY04] Qi Xie and Xiu Yuan Yu. Cryptanalysis of Tseng et al.'s authenticated encryption schemes. *Applied Mathematics and Computation*, 158(1):1–5, October 25, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Xu:2009:AVB

[XYL09] Songhua Xu, Wenxia Yang, and Francis C. M. Lau. Applications: a visualization based approach for digital signature authentication. *Computer Graphics Forum*, 28(3):935–942, June 2009. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Xing-Yuan:2011:PRS

[XYXYX11] Wang Xing-Yuan, Qin Xue, and Xie Yi-Xin. Pseudo-random sequences generated by a class of one-dimensional smooth map. *Chinese Physics Letters*, 28 (8):080501, 2011. CODEN CPLEEU. ISSN 0256-307X (print), 1741-3540 (electronic). URL http://stacks.iop.org/0256-307X/28/i=8/a=080501.

Yan:2000:NTC

[Yan00] S. Y. Yan. *Number Theory for Computing*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 0-387-65472-0. 256 (est.) pp. LCCN ???? US$46.00.

Yang:2002:NEC

[Yan02] Ching-Nung Yang. A note on efficient color visual encryption. *Journal of Information Science and Engineering*, 18(3):367–372, 2002. CODEN JINEEY. ISSN 1016-2364. Data encryption and cryptography.

Yang:2005:TFN

[Yan05] JiXian Yang. TWOBLOCK: a fast new hash function, 2005. URL http://yjxonline.hostrocket.com/Hash2005.pdf. World-Wide Web document.

Yan:2007:CAR

[Yan07] Song Y. Yan. *Cryptanalytic attacks on RSA*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 0-387-48741-7. xx + 254 pp. LCCN QA76.9.A25 Y34 2007.

Yasuda:2008:DLP

[Yas08] Masaya Yasuda. The discrete logarithm problem on elliptic curves defined over Q (abstract only). *ACM*

Communications in Computer Algebra, 42(1–2):64–66, March/June 2008. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Yuan-bo:2004:ITA

[YbJf04] Guo Yuan-bo and Ma Jianfeng. An intrusion-tolerant authorization and authentication scheme in distributed environments. *Operating Systems Review*, 38(4):45–51, October 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Yue:2001:GNN

[YC01] Tai-Wen Yue and Suchen Chiang. The general neural-network paradigm for visual cryptography. *Lecture Notes in Computer Science*, 2084:196–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2084/20840196.htm; http://link.springer-ny.com/link/service/series/0558/papers/2084/20840196.pdf.

Yue:2007:SEV

[YC07] Tai-Wen Yue and Suchen Chiang. The semipublic encryption for visual cryptography using Q'tron neural networks. *Journal of Network and Computer Applications*, 30(1):24–41, January 2007. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804505000391.

Yiu:2008:ODC

[YC08] Wai-Pun Ken Yiu and Shueng-Han Gary Chan. Offering data confidentiality for multimedia overlay multicast: Design and analysis. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 5(2):13:1–13:??, November 2008. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Yang:2009:ETP

[YC09a] Jen-Ho Yang and Chin-Chen Chang. An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments. *The Journal of Systems and Software*, 82(9):1497–1502, September 2009. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Yang:2009:IBR

[YC09b] Jen-Ho Yang and Chin-Chen Chang. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. *Computers & Security*, 28(3–4):138–143, May/June 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404808001120`.

Yang:2009:CGA

[YC09c] Seung S. Yang and Hongsik Choi. A complement to the GridOne authentication method. *Network Security*, 2009(12):12–18, December 2009. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485810700076`.

Yang:2004:MSS

[YCH04] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang Hwang. A (t, n) multi-secret sharing scheme. *Applied Mathematics and Computation*, 151(2):483–490, April 5, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yu:2007:NSM

[YCL07] Yuan-Hui Yu, Chin-Chen Chang, and Iuon-Chang Lin. A new steganographic method for color and grayscale image hiding. *Computer Vision and Image Understanding: CVIU*, 107(3):183–194, September 2007. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic).

Yang:2008:NFD

[YCW+08] Guomin Yang, Jing Chen, Duncan S. Wong, Xiaotie Deng, and Dongsheng Wang. A new framework for the design and analysis of identity-based identification schemes. *Theoretical Computer Science*, 407(1–3):370–388, November 6, 2008. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Yang:2007:IIS

[YCYW07] Ching-Nung Yang, Tse-Shih Chen, Kun Hsuan Yu, and Chung-Chun Wang. Improvements of image sharing with steganography and authentication. *The Journal of Systems and Software*, 80(7):1070–1076, July 2007. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Yung:2006:PKC

[YDKM06] Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors. *Public Key Cryptography: PPK 2006: 9th International Conference on Theory and Practice in Public-Key Cryp-*

tography, New York, NY, USA, April 24–26, 2006. Proceedings, volume 3958 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-540-33851-9 (softcover). LCCN ???? URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3958`.

Yekhanin:2007:LDC

[Yek07] Sergey Yekhanin. *Locally Decodable Codes and Private Information Retrieval Schemes*. Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA, 2007. URL `http://www.acm.org/press-room/news-releases/dd-award-07`. Winner of the ACM 2007 Doctoral Dissertation Award.

Yan:2006:ICP

[YEP+06] Chenyu Yan, Daniel Englender, Milos Prvulovic, Brian Rogers, and Yan Solihin. Improving cost, performance, and security of memory encryption and authentication. *ACM SIGARCH Computer Architecture News*, 34(2): 179–190, 2006. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Youssef:2001:CIM

[YG01a] A. Youssef and G. Gong. Cryptanalysis of Imai and Matsumoto scheme B asymmetric cryptosystem. *Lecture Notes in Computer Science*, 2247:214–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470214.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470214.pdf`.

Youssef:2001:IAB

[YG01b] A. M. Youssef and G. Gong. On the interpolation attacks on block ciphers. *Lecture Notes in Computer Science*, 1978:109–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780109.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780109.pdf`.

Youssef:2001:CPK

[YG01c] Amr Youssef and Guang Gong. Cryptanalysis of a public key cryptosystem proposed at ACISP 2000. *Lecture Notes in Computer Science*, 2119: 15–??, 2001. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190015.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190015.pdf.

Yang:2005:IME

[YGZ05] Jun Yang, Lan Gao, and Youtao Zhang. Improving memory encryption performance in secure processors. *IEEE Transactions on Computers*, 54(5): 630–640, May 2005. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1407851.

Yamamura:2000:QCB

[YI00] Akihiro Yamamura and Hirokazu Ishizuka. Quantum cryptanalysis of block ciphers. *Sūrikaisekikenkyūsho Kōkyūroku*, 1166:235–243, 2000. Algebraic systems, formal languages and computations (Japanese) (Kyoto, 2000).

Yamamura:2001:EDA

[YI01] Akihiro Yamamura and Hirokazu Ishizuka. Error detection and authentication in quantum key distribution. *Lecture Notes in Computer Science*, 2119: 260–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190260.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190260.pdf.

Yi:2004:AKA

[Yi04] Xun Yi. Authenticated key agreement in dynamic peer groups. *Theoretical Computer Science*, 326(1–3): 363–382, October 20, 2004. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Yen:2000:CBO

[YJ00] Sung-Ming Yen and M. Joye. Checking before output may not be enough against fault-based cryptanalysis. *IEEE Transactions on Computers*, 49(9):967–970, September 2000. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=869328.

Yen:2002:CAO

[YKLM02a] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sangjae Moon. A countermeasure against one physical cryptanalysis may benefit another attack. *Lecture*

Notes in Computer Science, 2288:414–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880414.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880414.pdf`.

Yen:2002:RSR

[YKLM02b] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sangjae Moon. RSA speedup with residue number system immune against hardware fault cryptanalysis. *Lecture Notes in Computer Science*, 2288:397–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880397.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880397.pdf`.

Yen:2003:RSC

[YKLM03] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sang-Jae Moon. RSA speedup with Chinese Remainder Theorem immune against hardware fault cryptanalysis. *IEEE Transactions on Computers*, 52 (4):461–472, April 2003. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1190587`.

Yardi:2008:HAC

[YKMB08] Sarita Yardi, Pamela Krolikowski, Taneshia Marshall, and Amy Bruckman. An HCI approach to computing in the real world. *ACM Journal on Educational Resources in Computing (JERIC)*, 8(3):9:1–9:??, October 2008. CODEN ???? ISSN 1531-4278.

Yamamoto:2001:PKB

[YKMY01] Hideo Yamamoto, Tetsutaro Kobayashi, Masahiro Morita, and Ryuji Yamada. Public-key-based high-speed payment (electronic money) system using contact-less smart cards. *Lecture Notes in Computer Science*, 2140:242–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2140/21400242.htm; http://link.springer-ny.com/link/service/series/0558/papers/2140/21400242.pdf`.

Yu:2001:TCB

[YKW01] Heather Yu, Xiangyang Kong, and Wayne Wolf.

Techniques for content-based graph authentication. *IEEE MultiMedia*, 8(4):38–45, October 2001. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://dlib.computer.org/mu/books/mu2001/pdf/u4038.pdf; http://www.computer.org/multimedia/mu2001/u4038abs.htm.

Yi:2009:SSG

[YLC+09] Ke Yi, Feifei Li, Graham Cormode, Marios Hadjieleftheriou, George Kollios, and Divesh Srivastava. Small synopses for group-by query verification on outsourced data streams. *ACM Transactions on Database Systems*, 34(3):15:1–15:??, August 2009. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Yu:2005:EHI

[YLH05] Jia Yu, Daxing Li, and Rong Hao. An efficient hierarchical ID-based signature scheme. In Han et al. [HYZ05b], pages 92–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Yoo:2002:LAU

[YLLL02] Hyejoung Yoo, Kwangsoo Lee, Sangjin Lee, and Jongin Lim. Off-line authentication using watermarks. *Lecture Notes in Computer Science*, 2288: 200–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2288/22880200.htm; http://link.springer-ny.com/link/service/series/0558/papers/2288/22880200.pdf.

Yurkewych:2005:CIR

[YLR05] Matthew Yurkewych, Brian N. Levine, and Arnold L. Rosenberg. On the cost-ineffectiveness of redundancy in commercial P2P computing. In Meadows and Syverson [MS05b], pages 280–288. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Yue:2006:NCB

[YLT06] Yao Yue, Chuang Lin, and Zhangxi Tan. NPCryptBench: a cryptographic benchmark suite for network processors. *ACM SIGARCH Computer Architecture News*, 34(1):49–56, 2006. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Young:2001:RP

[YN01] John Young and Deborah Natsios. Reversing the panopticon, 2001. Unpublished invited talk, Tenth

USENIX Security Symposium, August 13–17, 2001, Washington, DC, USA.

Youssef:2001:CAF

[You01] A. M. Youssef. Cryptanalysis of the "Augmented Family of Cryptographic Parity Circuits" proposed at ISW'97. *Lecture Notes in Computer Science*, 2012: 29–38, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120029.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120029.pdf.

Young:2004:HRV

[You04] Dale Young. Human resources have a vital role to play within employee identity and access management. *Network Security*, 2004(11):5–7, November 2004. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485804001540.

Young:2006:MCC

[You06] Anne L. Young. *Mathematical ciphers: from Caesar to RSA*, volume 25 of *Mathematical world*. American Mathematical Society, Providence, RI, USA, 2006. ISBN 0-8218-3730-3. viii + 159 pp. LCCN ????

Youn:2008:WRB

[YPKL08] Taek-Young Youn, Young-Ho Park, Changhan Kim, and Jongin Lim. Weakness in a RSA-based password authenticated key exchange protocol. *Information Processing Letters*, 108(6):339–342, November 30, 2008. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Yang:2009:AIO

[YPPK09] Yin Yang, Stavros Papadopoulos, Dimitris Papadias, and George Kollios. Authenticated indexing for outsourced spatial databases. *VLDB Journal: Very Large Data Bases*, 18(3):631–648, June 2009. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Yin:2001:RMW

[YPSZ01] Kangkang Yin, Zhigeng Pan, Jiaoying Shi, and David Zhang. Robust mesh watermarking based on multiresolution processing. *Computers and Graphics*, 25(3):409–420, June 2001. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.elsevier.nl/gej-ng/10/13/20/57/32/

32/abstract.html; http://www.elsevier.nl/gej-ng/10/13/20/57/32/32/article.pdf.

Yilek:2009:WPK

[YRS+09] Scott Yilek, Eric Rescorla, Hovav Shacham, Brandon Enright, and Stefan Savage. When private keys are public: Results from the 2008 Debian OpenSSL vulnerability. In ????, editor, *ACM Internet Measurement Conference*, page ?? ACM Press, New York, NY 10036, USA, 2009. ISBN ???? LCCN ???? URL ????.

Yoon:2004:SUA

[YRY04] Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo. A secure user authentication scheme using hash functions. *Operating Systems Review*, 38(2):62–68, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Yoon:2005:CFI

[YRY05a] Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo. Cryptanalysis and further improvement of Peinado's improved LHL-key authentication scheme. *Applied Mathematics and Computation*, 168(2):788–794, September 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yoon:2005:ICJ

[YRY05b] Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo. Improvement of Chien–Jan's authenticated multiple-key agreement protocol without using conventional one-way function. *Applied Mathematics and Computation*, 167(1):711–715, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yoon:2005:IFA

[YRY05c] Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo. Improvement of Fan et al.'s deniable authentication protocol based on Diffie–Hellman algorithm. *Applied Mathematics and Computation*, 167(1):274–280, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yoon:2005:IHL

[YRY05d] Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo. An improvement of Hwang–Lee–Tang's simple remote user authentication scheme. *Computers & Security*, 24 (1):50–56, February 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001749.

Yeh:2002:SAK

[YS02] Her-Tyan Yeh and Hung-Min Sun. Simple authenticated key agreement protocol resistant to password guessing attacks. *Operating Systems Review*, 36(4):14–22, October 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Yeh:2004:PBU

[YS04] Her-Tyan Yeh and Hung-Min Sun. Password-based user authentication and key distribution protocols for client–server applications. *The Journal of Systems and Software*, 72(1):97–103, June 2004. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Yanami:2002:DLC

[YSD02] Hitoshi Yanami, Takeshi Shimoyama, and Orr Dunkelman. Differential and linear cryptanalysis of a reduced-round SC2000. *Lecture Notes in Computer Science*, 2365:34–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650034.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650034.pdf.

Yeh:2003:IAM

[YSH03] Her-Tyan Yeh, Hung-Min Sun, and Tzonelih Hwang. Improved authenticated multiple-key agreement protocol. *Computers and Mathematics with Applications*, 46(2–3):207–211, July/August 2003. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122103900253.

Yang:2001:EEA

[YSR01] Jong-Phil Yang, Weon Shin, and Kyung-Hyune Rhee. An end-to-end authentication protocol in wireless application protocol. *Lecture Notes in Computer Science*, 2119:247–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190247.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190247.pdf.

Yoshiura:2001:AWB

[YSS+01] Hiroshi Yoshiura, Takaaki Shigematsu, Seiichi Susaki, Tsukasa Saitoh, Hisashi

Toyoshima, Chikako Kurita, Satoru Tezuka, and Ryoichi Sasaki. Authenticating Web-based virtual shops using signature-embedded marks — A practical analysis. *Lecture Notes in Computer Science*, 2133: 238–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2133/21330238.htm; http://link.springer-ny.com/link/service/series/0558/papers/2133/21330238.pdf.

Yao:2009:CAR

[YT09] Danfeng Yao and Roberto Tamassia. Compact and anonymous role-based authorization chain. *ACM Transactions on Information and System Security*, 12(3):15:1–15:??, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Yang:2004:ENT

[YTH04] Cheng-Ying Yang, Shiang-Feng Tzeng, and Min-Shiang Hwang. On the efficiency of nonrepudiable threshold proxy signature scheme with known signers. *The Journal of Systems and Software*, 73(3):507–514, November/December 2004. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Ytrehus:2006:CCI

[Ytr06] Øyvind Ytrehus, editor. *Coding and Cryptography: International Workshop, WCC 2005, Bergen, Norway, March 14–18, 2005. Revised Selected Papers*, volume 3969 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Yang:2005:SEA

[YTWY05] Chou-Chen Yang, Yuan-Liang Tang, Ren-Chiun Wang, and Hung-Wen Yang. A secure and efficient authentication protocol for anonymous channel in wireless communications. *Applied Mathematics and Computation*, 169(2):1431–1439, October 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yung:2002:ACC

[Yun02a] Moti Yung, editor. *Advances in cryptology — CRYPTO 2002: 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18–22, 2002: Proceedings*, volume 2442 of *Lecture*

Notes in Computer Science and Lecture Notes in Artificial Intelligence. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442.

Yung:2002:CI

[Yun02b] Moti Yung. Crypto-integrity. *Lecture Notes in Computer Science*, 2501: 567–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010567.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010567.pdf.

Yang:2004:ISE

[YW04a] Chou-Chen Yang and Ren-Ching Wang. An improvement of security enhancement for the timestamp-based password authentication scheme using Smart Cards. *Operating Systems Review*, 38(3):91–96, July 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Yang:2004:CUF

[YW04b] Chou-Chen Yang and Ren-Chiun Wang. Cryptanalysis of a user friendly remote authentication scheme with smart cards. *Computers & Security*, 23(5):425–427, July 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804001002.

Yang:2005:CIA

[YW05] Chou-Chen Yang and Ren-Chiun Wang. Cryptanalysis of improved authenticated multiple-key agreement protocol without using conventional one-way function. *Applied Mathematics and Computation*, 162 (1):211–214, March 4, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yen:2006:SED

[YW06] Chih-Hsu Yen and Bing-Fei Wu. Simple error detection methods for hardware implementation of Advanced Encryption Standard. *IEEE Transactions on Computers*, 55(6):720–731, June 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-

9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1628959.

Yang:2005:IYS

[YWC05] Chou-Chen Yang, Ren-Chiun Wang, and Ting-Yi Chang. An improvement of the Yang-Shieh password authentication schemes. *Applied Mathematics and Computation*, 162(3):1391–1396, March 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yang:2008:VCS

[YWC08] Ching-Nung Yang, Chung-Chun Wang, and Tse-Shih Chen. Visual cryptography schemes with reversing. *The Computer Journal*, 51(6):710–722, November 2008. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/51/6/710; http://comjnl.oxfordjournals.org/cgi/content/full/51/6/710; http://comjnl.oxfordjournals.org/cgi/reprint/51/6/710.

Yang:2008:FSD

[YWD08] G. Yang, D. S. Wong, and X. Deng. Formal security definition and efficient construction for roaming with a privacy-preserving extension. *J.UCS: Journal of Universal Computer Science*, 14(3):441–462, ???? 2008. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_14_3/formal_security_definition_and.

Yang:2005:SAS

[YWL05] Chou-Chen Yang, Ren-Chiun Wang, and Wei-Ting Liu. Secure authentication scheme for session initiation protocol. *Computers & Security*, 24(5):381–386, August 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804002640.

Yang:2008:TFM

[YWWD08] Guomin Yang, Duncan S. Wong, Huaxiong Wang, and Xiaotie Deng. Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences*, 74(7):1160–1172, November 2008. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000008000482.

Yang:2009:CLW

[YWWS09] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng

Wang, and Hung-Min Sun. Codebook-linked watermarking scheme for digital images. *Fundamenta Informaticae*, 92(4):397–409, June 2009. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Young:2000:RBA

[YY00] Adam Young and Moti Yung. RSA-based auto-recoverable cryptosystems. *Lecture Notes in Computer Science*, 1751:326–341, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Young:2001:BOK

[YY01] A. Young and M. Yung. Bandwidth-optimal kleptographic attacks. *Lecture Notes in Computer Science*, 2162:235–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620235.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620235.pdf.

Young:2004:MCE

[YY04] Adam Young and Moti Yung. *Malicious cryptography: exposing cryptovirology*. John Wiley and Sons, Inc., New York, NY, USA, 2004. ISBN 0-7645-4975-8 (paperback). xxiv + 392 pp. LCCN QA76.9.A25 Y65 2004. URL http://www.loc.gov/catdir/bios/wiley047/2003023863.html; http://www.loc.gov/catdir/description/wiley041/2003023863.html; http://www.loc.gov/catdir/toc/wiley041/2003023863.html.

Yoon:2005:CZX

[YY05a] Eun-Jun Yoon and Kee-Young Yoo. Cryptanalysis of Zhang–Xiao's multisignature scheme for specified group of verifiers. *Applied Mathematics and Computation*, 170(1):226–229, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yoon:2005:SWL

[YY05b] Eun-Jun Yoon and Kee-Young Yoo. On the security of Wu-Lin's robust key authentication scheme. *Applied Mathematics and Computation*, 169(1):1–7, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Ye:2001:ATD

[YYDO01] Dingfeng Ye, Junhui Yang, Zongduo Dai, and Haiwen Ou. Attacks on two digital signature schemes based on error correcting codes. *Lecture Notes in Computer Science*, 2229:84–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290084.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290084.pdf.

You:2001:GEC

[YYZ01] Lin You, Yi Xian Yang, and Chun Qi Zhang. Generalization of elliptic curve digital signature schemes. *Lecture Notes in Computer Science*, 2229:246–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290246.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290246.pdf.

Yen:2000:WOW

[YZ00] Sung-Ming Yen and Yuliang Zheng. Weighted one-way hash chain and its applications. *Lecture Notes in Computer Science*, 1975:135–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750135.htm; http://link.springer-ny.com/link/service/series/0558/papers/1975/19750135.pdf.

Ye:2007:NAW

[YZDW07] Dengpan Ye, Changfu Zou, Yuewei Dai, and Zhiquan Wang. A new adaptive watermarking for real-time MPEG videos. *Applied Mathematics and Computation*, 185(2):907–918, February 15, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Youssef:2009:IEU

[YZEE09] M. I. Youssef, M. Zahara, A. E. Emam, and M. A. Elghany. Image encryption using pseudo random number and chaotic sequence generators. In *NRSC 2009. National Radio Science Conference, 2009*, pages 1–15. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5233974.

Zafar:2000:ACB

[Zaf00] Naeem Zafar. Authentication company buys smart card firm. *Network Security*, 2000(5):4–5, May 1, 2000. CODEN

NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348580005011X.

Zane:2001:EWD

[Zan01] Francis Zane. Efficient watermark detection and collusion security. *Lecture Notes in Computer Science*, 1962:21–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1962/19620021.htm; http://link.springer-ny.com/link/service/series/0558/papers/1962/19620021.pdf.

Zhang:2005:ITA

[ZAX05] Zhang Zhang, Shunsuke Araki, and Guozhen Xiao. Improvement of Tseng et al.'s authenticated encryption scheme with message linkages. *Applied Mathematics and Computation*, 162 (3):1475–1483, March 25, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Zivkovic:2005:AAH

[ŽBLvB05] Miroslav Živković, Milind M. Buddhikot, Ko Lagerberg, and Jeroen van Bemmel. Authentication across heterogeneous networks. *Bell Labs Technical Journal*, 10 (2):39–56, Summer 2005. CODEN BLTJFD. ISSN 1089-7089 (print), 1538-7305 (electronic).

Zhao:2005:SSV

[ZBP05] Xin Zhao, Kevin Borders, and Atul Prakash. SVGrid: a secure virtual environment for untrusted grid applications. In ACM [ACM05a], pages 1–6. ISBN 1-59593-269-0. LCCN ????

Zhang:2000:MCA

[ZC00] Muxiang Zhang and Agnes Chan. Maximum correlation analysis of nonlinear S-boxes in stream ciphers. In Bellare [Bel00], pages 501–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800501.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800501.pdf.

Zhang:2004:AIB

[ZC04] Fangguo Zhang and Xiaofeng Chen. Attack on an ID-based authenticated group key agreement scheme from PKC 2004. *Information Processing Letters*, 91 (4):191–193, August 2004. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Zhang:2005:CHC

[ZC05] Fangguo Zhang and Xiaofeng Chen. Cryptanalysis of Huang–Chang partially blind signature scheme. *The Journal of Systems and Software*, 76(3):323–325, June 2005. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Zhang:2009:CII

[ZC09] Fangguo Zhang and Xiaofeng Chen. Cryptanalysis and improvement of an ID-based ad-hoc anonymous identification scheme at CT-RSA 05. *Information Processing Letters*, 109 (15):846–849, July 16, 2009. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Zhang:2001:SOS

[ZCC01] Muxiang Zhang, Christopher Carroll, and Agnes Chan. The software-oriented stream cipher SSC2. *Lecture Notes in Computer Science*, 1978: 31–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780031.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780031.pdf.

Zhou:2005:PSP

[ZCL05] Yuan Zhou, ZhenFu Cao, and RongXing Lu. Provably secure proxy-protected signature schemes based on factoring. *Applied Mathematics and Computation*, 164(1):83–98, May 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Zhu:2004:DSM

[ZCW04] Lie Huang Zhu, Yuan Da Cao, and Dong Wang. Digital signature of multicast streams secure against adaptive chosen message attack. *Computers & Security*, 23(3):229–240, May 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404804000707.

Zunino:2005:WPE

[ZD05] Roberto Zunino and Pierpaolo Degano. Weakening the perfect encryption assumption in Dolev–Yao adversaries. *Theoretical Computer Science*, 340(1):154–178, June 13, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Zhao:2006:SAP

[ZDW06] Zhu Zhao, Zhongqi Dong, and Yongge Wang. Security analysis of a password-based authentication protocol proposed to IEEE 1363. *Theoretical Computer Science*, 352(1–3):280–287, March 7, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Zeadally:2000:IPQ

[Zea00] S. Zeadally. Implementation and performance of QoS-aware Java applications over ATM networks. *The Computer Journal*, 43 (4):266–273, ???? 2000. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_43/Issue_04/430266.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_43/Issue_04/pdf/430266.pdf.

Zhang:2005:CSS

[ZF05] Zhenfeng Zhang and Dengguo Feng. Cryptanalysis of some signature schemes with message recovery. *Applied Mathematics and Computation*, 170(1): 103–114, November 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Zhen:2004:IBS

[ZFK04] Z. Zhen, B. Fei, and L. Kejun. The implementation of 128 bit strong encryption for SSL by using Java applet. *Journal — Huazhong University of Science and Technology Nature Science Chinese Edition*, 32(4):74–76, 2004. CODEN ???? ISSN 1671-4512.

Zhang:2005:AES

[ZGLX05] Zhikun Zhang, Youping Geng, Tingyan Li, and Jianguo Xiao. Analysis of enhanced separation of duty in role-based access control model. In Han et al. [HYZ05b], pages 69–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Zou:2005:MED

[ZGTG05] Cliff C. Zou, Weibo Gong, Don Towsley, and Lixin Gao. The monitoring and early detection of Internet worms. *IEEE/ACM Transactions on Networking*, 13 (5):961–974, October 2005. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Zhang:2000:WMH

[Zha00] Peter Zhang. Webrelay: a multithreaded HTTP relay server. *Dr. Dobb's Journal of Software Tools*, 25(2):86, 88, 90–94, 96, February 2000. CODEN DDJOEB. ISSN

1044-789X. URL http://www.ddj.com/ftp/2000/2000_02/webrelay.txt; http://www.ddj.com/ftp/2000/2000_02/webrelay.zip.

Zhao:2006:NDN

[Zha06] Yunlei Zhao. A note on the Dwork–Naor timed deniable authentication. *Information Processing Letters*, 100 (1):1–7, October 16, 2006. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Zhang:2008:CLR

[Zha08] Yu Zhang. Cryptographic logical relations. *Theoretical Computer Science*, 394(1–2):39–63, March 31, 2008. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Zheng:2001:ISS

[Zhe01] Yuliang Zheng. Identification, signature and signcryption using high order residues modulo an RSA composite. *Lecture Notes in Computer Science*, 1992:48–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1992/19920048.htm; http://link.springer-ny.com/link/service/series/0558/papers/1992/19920048.pdf.

Zheng:2002:NPK

[Zhe02a] Jiande Zheng. A new public key cryptosystem for constrained hardware. *Lecture Notes in Computer Science*, 2433:334–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330334.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330334.pdf.

Zheng:2002:ACA

[Zhe02b] Yuliang Zheng, editor. *Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1–5, 2002. Proceedings*, volume 2501 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-00171-9 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 2002. URL http://link.springer-ny.com/link/service/series/0558/

tocs/t2501.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2501. Also available via the World Wide Web.

Zhou:2002:MVD

[Zho02] Jianying Zhou. Maintaining the validity of digital signatures in B2B applications. *Lecture Notes in Computer Science*, 2384: 303–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840303.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840303.pdf.

Zhong:2006:ESC

[Zho06] Sheng Zhong. An efficient and secure cryptosystem for encrypting long messages. *Fundamenta Informaticae*, 71(4):493–497, September 2006. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Zirkind:2007:ADC

[Zir07] Givon Zirkind. AFIS data compression: an example of how domain specific compression algorithms can produce very high compression ratios. *Computer Graphics*, 41(4):1–36, November 2007. CODEN CGRADI, CPGPBZ. ISSN 0097-8930 (print), 1558-4569 (electronic).

Zhang:2004:BAF

[ZJ04] David Zhang and Anil K. Jain, editors. *Biometric Authentication: First International Conference, ICBA 2004, Hong Kong, China, July 15–17, 2004, Proceedings*, volume 3072 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22146-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76 A1 L43 3072 (LC). URL http://link.springer-ny.com/link/service/series/0558/tocs/t3072.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3072; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b98225.

Zhang:2009:IBR

[ZJ09] Jianhong Zhang and Cheng Ji. An id-based and repairing NTRUSign-based anonymous multi-proxy signature scheme. In IEEE, editor, *Proceedings of the International Conference on Computational Intelligence and Software Engineering,* *2009. CiSE 2009, December 11–13, 2009, Wuhan, China*, pages 1–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. ISBN 1-4244-4507-8. LCCN QA76.758 2009. URL http://ieeexplore.ieee.org/servlet/opac?punumber=5362500. IEEE catalog number CFP0926H.

Zhang:2002:IBB

[ZK02] Fangguo Zhang and Kwangjo Kim. ID-based blind signature and ring signature from pairings. *Lecture Notes in Computer Science*, 2501: 533–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2501/25010533.htm; http://link.springer.de/link/service/series/0558/papers/2501/25010533.pdf.

Zhang:2005:CLH

[ZK05] Fangguo Zhang and Kwangjo Kim. Cryptanalysis of Lee–Hwang–Li's key authentication scheme. *Applied Mathematics and Computation*, 161(1):101–107, February 4, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). See comment [SCS05b].

Zenner:2001:ICS

[ZKL01] Erik Zenner, Matthias Krause, and Stefan Lucks. Improved cryptanalysis of the self-shrinking generator. *Lecture Notes in Computer Science*, 2119: 21–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190021.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190021.pdf.

Zhang:2004:SAE

[ZL04a] Chang N. Zhang and Chunren Lai. A systematic approach for encryption and authentication with fault tolerance. *Computer Networks (Amsterdam, Netherlands: 1999)*, 45(2):143–154, June 5, 2004. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Zhang:2004:AFV

[ZL04b] Yuqing Zhang and Xiuying Liu. An approach to the formal verification of the three-principal cryptographic protocols. *Operating Systems Review*, 38(1):35–42, January 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Zhang:2004:RMA

[ZL04c] Yuqing Zhang and Xiuying Liu. Running-mode analysis of the Security Socket Layer protocol. *Operating Systems Review*, 38(2):34–40, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Zhao:2005:MCE

[ZL05] Ze-Mao Zhao and Feng-Yu Liu. Method of constructing elliptic curve authenticated encryption scheme. *Applied Mathematics and Computation*, 168(1):146–151, September 1, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Zhang:2001:QKD

[ZLG01] Yong-Sheng Zhang, Chuan-Feng Li, and Guang-Can Guo. Quantum key distribution via quantum encryption. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 64(2):024302, 4, 2001. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519.

Zhang:2002:CRD

[ZLK02] Fangguo Zhang, Shengli Liu, and Kwangjo Kim. Compact representation of domain parameters of hyperelliptic curve cryptosystems. *Lecture Notes in Computer Science*, 2384:203–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840203.htm; http://link.springer-ny.com/link/service/series/0558/papers/2384/23840203.pdf`.

Zhang:1999:AFV

[ZLX99] Yuqing Zhang, Jihong Li, and Guozhen Xiao. An approach to the formal verification of the two-party cryptographic protocols. *Operating Systems Review*, 33(4):48–51, October 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic). See comments [JW01].

Zheng:2007:SRI

[ZLZS07] Dong Zheng, Yan Liu, Jiying Zhao, and Abdulmotaleb El Saddik. A survey of RST invariant image watermarking algorithms. *ACM Computing Surveys*, 39(2):5:1–5:91, July 2007. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Zolman:2001:SEM

[Zol01] Leor Zolman. An STL error message decryptor for Visual C++. *C/C++ Users Journal*, 19(7):24–??, July

2001. CODEN CCUJEX. ISSN 1075-2838.

Zhang:2001:CIS

[ZP01] Xian-Mo Zhang and Josef Pieprzyk. Cheating immune secret sharing. *Lecture Notes in Computer Science*, 2229:144–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290144.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290144.pdf.

Zhang:2005:DMC

[ZP05] Zhiyong Zhang and Jiexin Pu. Delegation model for CSCW based on RBAC policies and visual modeling. In Han et al. [HYZ05b], pages 126–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Zhou:2005:MBI

[ZS05] Zhenyu Zhou and Jianjing Shen. Multiagent-based information fusion model for network security. In Han et al. [HYZ05b], pages 139–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Zhu:2007:IHH

[ZSJN07] Sencun Zhu, Sanjeev Setia, Sushil Jajodia, and Peng Ning. Interleaved hop-by-hop authentication against false data injection attacks in sensor networks. *ACM Transactions on Sensor Networks*, 3(3):14:1–14:??, August 2007. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Zhang:2005:RPE

[ZSM05] N. Zhang, Q. Shi, and M. Merabti. Revocation of privacy-enhanced public-key certificates. *The Journal of Systems and Software*, 75(1–2):205–214, February 15, 2005. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Zhao:2005:APA

[ZSN05] Meiyuan Zhao, Sean W. Smith, and David M. Nicol. Aggregated path authentication for efficient BGP security. In Meadows and Syverson [MS05b], pages 128–138. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Zhou:2005:APS

[ZSV05] Lidong Zhou, Fred B. Schneider, and Robbert Van Renesse. APSS: proactive secret sharing in asynchronous systems. *ACM*

Transactions on Information and System Security, 8 (3):259–286, August 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhang:2001:ASE

[ZSZ01] Long Jun Zhang, Jun Yi Shen, and Lin Zhao. An approach to the security of elliptic curve cryptosystems. *Xi'an Jiaotong Daxue Xuebao*, 35(10):1038–1041, 1058, 2001. CODEN HCTPDW. ISSN 0253-987X.

Zhang:2003:FSP

[ZT03] Zhenxiang Zhang and Min Tang. Finding strong pseudoprimes to several bases. II. *Mathematics of Computation*, 72(244):2085–2097, October 2003. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/journal-getitem?pii=S0025-5718-03-01545-X`; `http://www.ams.org/mcom/2003-72-244/S0025-5718-03-01545-X/S0025-5718-03-01545-X.dvi`; `http://www.ams.org/mcom/2003-72-244/S0025-5718-03-01545-X/S0025-5718-03-01545-X.pdf`; `http://www.ams.org/mcom/2003-72-244/S0025-5718-03-01545-X/S0025-5718-03-01545-X.ps`; `http://www.ams.org/mcom/2003-72-244/S0025-5718-03-01545-X/S0025-5718-03-01545-X.tex`.

Zafeiriou:2005:BRW

[ZTP05] Stefanos Zafeiriou, Anastasios Tefas, and Ioannis Pitas. Blind robust watermarking schemes for copyright protection of 3D mesh objects. *IEEE Transactions on Visualization and Computer Graphics*, 11(5):596–607, September/October 2005. CODEN ITVGEA. ISSN 1077-2626 (print), 1941-0506 (electronic), 2160-9306.

Zhang:2005:ISS

[ZW05a] Jianhong Zhang and Yumin Wang. An improved signature scheme without using one-way Hash functions. *Applied Mathematics and Computation*, 170(2):905–908, November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Zhang:2005:SCA

[ZW05b] Jianhong Zhang and Yumin Wang. On the security of a convertible authenticated encryption. *Applied Mathematics and Computation*, 169(2):1063–1069, October 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Zhao:2002:EII

[ZWC02] Xianfeng Zhao, Weinong Wang, and Kefei Chen. Exploiting the intrinsic irreversibility of adaptive technologies to enhance the security of digital watermarking. *Lecture Notes in Computer Science*, 2419: 430–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2419/24190430.htm; http://link.springer-ny.com/link/service/series/0558/papers/2419/24190430.pdf.

Zhu:2002:PAK

[ZWCY02] Feng Zhu, Duncan S. Wong, Agnes H. Chan, and Robbie Ye. Password authenticated key exchange based on RSA for imbalanced wireless networks. *Lecture Notes in Computer Science*, 2433:150–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330150.htm; http://link.springer-ny.com/link/service/series/0558/papers/2433/24330150.pdf.

Zhang:2001:USC

[ZWWL01] Yuqing Zhang, Chunling Wang, Jianping Wu, and Xing Li. Using SMV for cryptographic protocol analysis: a case study. *Operating Systems Review*, 35(2): 43–50, April 2001. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Zhang:2004:NMS

[ZX04] Zhang Zhang and Guozhen Xiao. New multisignature scheme for specified group of verifiers. *Applied Mathematics and Computation*, 157(2):425–431, October 5, 2004. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Zhong:2008:GPT

[ZY08] Sheng Zhong and Zhiqiang Yang. Guided perturbation: towards private and accurate mining. *VLDB Journal: Very Large Data Bases*, 17 (5):1165–1177, August 2008. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Zhou:2003:ACN

[ZYH03] Jianying Zhou, Moti Yung, and Yongfei Han, editors. *Applied Cryptography and Network Security: First Title: International Conference, ACNS 2003, Kunming, China, October 16–19, 2003: Proceedings*, volume 2846 of *Lecture Notes in Computer*

Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-20208-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK5102.94 .A28 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2846.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2846; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b13996.

Zhang:2005:ASP

[ZYLG05] Youtao Zhang, Jun Yang, Yongjing Lin, and Lan Gao. Architectural support for protecting user privacy on trusted processors. *ACM SIGARCH Computer Architecture News*, 33(1):118–123, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Zhang:2005:ISM

[ZYM05] Peng Zhang, Chengqing Ye, and Xueying Ma. Improvement of secure mobile agent system in electronic commerce. In Han et al. [HYZ05b], pages 114–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

Zhang:2008:FIC

[ZYN08] Qing Zhang, Ting Yu, and Peng Ning. A framework for identifying compromised nodes in wireless sensor networks. *ACM Transactions on Information and System Security*, 11(3):12:1–12:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zeng:2001:CHR

[ZYR01] Kencheng Zeng, Chung-Huang Yang, and T. R. N. Rao. Cryptanalysis of the Hwang-Rao secret error-correcting code schemes. *Lecture Notes in Computer Science*, 2229:419–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2229/22290419.htm; http://link.springer-ny.com/link/service/series/0558/papers/2229/22290419.pdf.

Zhu:2007:EIB

[ZYW07] Robert W. Zhu, Guomin Yang, and Duncan S. Wong. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices. *Theoretical Computer Science*, 378

(2):198–207, June 6, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Zhuang:2005:KAE

[ZZT05] Li Zhuang, Feng Zhou, and J. D. Tygar. Keyboard acoustic emanations revisited. In Meadows and Syverson [MS05b], pages 373–382. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.