A Bibliography of Publications on Cryptography: 1990–1999

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/

02 November 2023
Version 1.110

Title word cross-reference

De 93a, HRT96, IH99b, Kay95, Koh90, KN93, KNT94, Lei99a, Lin96b, Lun90, Men91, NT94, Rus90, SA95, Sin95, Ste92, Ts'97, Tun99, Yu94a, Yu94b]. **Kernel** [BCCG93, WB92]. **Kerry** [IEE96c]. **KEY** [YY98d, ANS97, ANS98b, AKP96, AAB+97, AN95, IBM93, Ano94b, Ano94d, Ano94f, Ano95s, Ano97e, Ano99j, Ano99l, AA93, BP98a, BI95, BDHJ98, BDGI98, BCE+94, Bar96a, BCG90, BR94a, BR95b, BHSV98b, BHSV98a, BDPR98, Ber97c, BS91b, BS97a, Bir98, BMS94, BWM98, BWM99a, BWM99b, Bla94b, BDR+96, Bla96c, BPK99, BFK99, Ble97, BDHK93, BFS96, BDF98, BD99b, BF99c, Boy90, BM94b, Bra95b, Bra95c, BS94, Bur94b, BDS98, Cae96a, CC99b, CG99, CDN98, CJS91, CGM97a, CS98b, Cra98, Cus97, DDJ98g, DDJ98h, Dae98, Dam91b, DK96, Dan95, DDP90, Dav96, De 93c, DP98c, DB96, Dif90, DH90, ECM96, FW91, FDB93a, FY95a, FY98a, FYM99, FBS98, FO99a, Fum98c, Fun93, GHY90, Gal96, Gan96a, GJKR99, Gib91, Gib96, Gil99, GM90, GGH97b, Gys96, HK99a, HGS98]. **Key** [HP98a, HS90, HMT+98, HMV93, Haw98b, HD96b, HJJ+xx, Hes97, HPS98, HFPS99, HM98, HR90, Hwa97, Iss90, Jab90, Jas96, JV96, Kal99, KP99a, KSW96, KSW99a, Kel99, KS99b, KP96b, KM99c, KT91a, KMOV91, KKOT91, KP93, RSA93f, Lan99, LM94b, LWY95, LMS97, LA98, LP99, Low96, Luc98b, Mah96, Mar97, Mat91, MY91, Mau93a, MW96a, Mau97a, MP91, Mv93, Men93, MM96b, Mic93a, Mic93b, MS95f, MM99c, MS99c, MKS99, MSN98, MSN99, MTVZ92, MAO96, MM98a, MM98b, NMR95, NS97a, Nec96, Neu97, NS99a, Oka94, OU98a, Oka98a, Oka98b, Omu90, vO91a, PSR97, Pai99d, PKOT94, Pat95, Pin97, Poi99, PB99a, RSA93b, RSA93e, RSA94, ROT94, RS98c, RS98d, Ros96a, Ros96e, Ros96f, Ros97b, Ros98b, Ros98c, RCM99, SSN98a, SYMI98, Sam98, DP91, Sas99a, Sch94b, SKW+98a]. **Key** [SKWW99, SOOS95, SM95a, SE96, Sha99b, She94d, SiK93, SR96, Slu98, Sta99b, ST91, SW99b, SH94, Sun98a, Sut99, TAP90, TA92, Uni98i, Van95a, Van93, VSH97, VvT97, VBD99, WM93, dWQ91b, WLEB96, WW98b, WKS+99, Wie96, Wie97, Wie98a, Wie98b, Wol98, Yam98b, YST99a, YST99b, dWQ91a, vO91b, vOW96, AA95, Acc97, Lip98, AD97, AD99, Al 96, Ano90, Ano96q, Ano96o, Ano96w, Ano96-30, Ano97k, Ano97v, Ano98f, BSNP96a, BSNP96b, Bao94, BI94, BDHJ97, BD98a, BTD98, BSB97, BR96b, BCK98, BY93c, BY93b, BS91a, BFS92a, BGH+95a, BMP97a, BF96, Ble96, BMS96, BFS98, BM95, Boy97, Bur94a, BD95b, CC99a, CW97, Cle96, Cra97, Cus95, DKR97b, DWZ96, DS90a, DH96a, Des95, DVQ96, Dhe98, DvW92, DN95b, ES97, FDB93b, FGMY97a, FMY98, Fre94, Fro96]. **key** [FGLP96a, FGLP96b, FL93, Gar96b, GH96, Gib95, GBL94, GH99, GTS90, HNSM91, HP99a, HP99b, HY93b, HJT+96, Haw98a, He92, HWF96, HJJ+97, HI97, HY98b, HY98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IZ98, IZ99, JM96a, Jar96, JLM+94, Jon90, JY98, KASH90, KM99a, KSW97a, KSW97b, KL94, KR96b, Kir95, KM98c, Koo97, KM99d, Kos99, Kum97, LG97, Laš92, LMJW93, Lee95, LC96a, LM94a, LZ90, LZ91a, LDW94, LL95b, LCL95, Lon91, Lon92, Low95, Mad98f, MS98a, Mao97, MLA91, Mau91b, MY93b, MKKW99, Mu92, MLLG95, NM96a, NY90, Nat97a, Nec91, Odl94b, Ole95, PS98e, PS98f, Pet91, PP92b, RFLW96, RT93, Roe99, Sal90, Sal96, SW95a, Sch92c, Sha95a, She96a, She92c, SKB97, SY96b, SM90, Smi93b, SS95b, SS95c, STW95, Sun91a, SS98b, Syv93, SM95b, Tab94, Tao94, TCC97, TC97]. **key** [TC99b, TC99a, Ts'90, TC91, Tze99, TH99, Uni97c, Uni95a, VW96, Ven92, Wan92b, Wie94, Wil93b, Xie92, Xie93, XLP99, XW97, Yam98a, YL97b, Yu92, Zha91, Zhe95a, Zhe95b, ZPY96, vOW91,

References

Anonymous:1990:IWH

[???90] *IT Workshop, Hawaii, USA, November 27–30.* ????, ????, 1990.

Anonymous:1997:ACC

[???97] *1997 ACM Conference on Computers and Communication Security.* ????, ????, 1997.

ANSI:1988:FIE

[AA88] American National Standards Institute and American Bankers Association.Secretariat. *Financial institution encryption of wholesale financial messages: X9.23.* American Bankers Association, Washington, DC, USA, 1988. vii + 28 pp.

Anshel:1993:PMT

[AA93] Iris Lee Anshel and Michael Anshel. From the post-Markov theorem through decision problems to public-key cryptography. *American Mathematical Monthly*, 100(9):835–844, November 1993. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

ANSI:1995:ANS

[AA95] American National Standards Institute and American Bankers Association.

American National Standard for Financial Services: public key cryptography using irreversible algorithms for the financial services industry. part 1: The Digital Signature Algorithm (DSA). Report ANSI/X9.30-1995, Washington Publishing, Gaithersburg, MD, USA, May 26, 1995. vi + 18 pp. Approved May 26, 1995.

Arabnia:1997:ICI

[AA97] Hamid R. Arabnia and Farid Ahmed, editors. *International Conference on Imaging Science, Systems, and Technology: CISST '97: June 30–July 3, 1997, Las Vegas, Nevada, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. ISBN 0-9648666-9-2. LCCN ????

Abdikalikov:1999:ERC

[AA99] K. A. Abdikalikov and N. I. Abdikalikova. ElGamal and RSA cryptosystems and their comparative analysis. *Izv. Minist. Nauki Vyssh. Obraz. Resp. Kaz. Nats. Akad. Nauk Resp. Kaz. Ser. Fiz.-Mat.*, 3:3–8 (2000), 1999. ISSN 0002-3191.

Abelson:1997:RKR

[AAB+97] Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter C. Neumann, Ronald L. Rivest, Jeffrey Schiller, and Bruce Schneier. The risks of key recovery, key escrow, and trusted third-party encryption. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, May 27, 1997. 20 pp. URL `http://www.counterpane.com/key-escrow.html`.

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].

Andrasiu:1992:NCB

[AAPS92] Mircea Andraşiu, Adrian Atanasiu, Gheorghe Păun, and Arto Salomaa. A new cryptosystem based on formal language theory. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 36(84)(1):1–16, 1992. ISSN 1220-3874.

Asmuth:1981:EAC

[AB81] C. A. Asmuth and G. R. Blakley. An efficient algorithm for constructing a cryptosystem which is harder to break than two other cryptosystems. *Computers and Mathematics with Applications*, 7(6): 447–450, 1981. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Anderson:1996:TPP

[AB96a] R. Anderson and E. Biham. Two practical and provably secure block ciphers: Bear and lion. *Lecture Notes in Computer Science*, 1039: 113–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anderson:1996:TFN

[AB96b] Ross Anderson and Eli Biham. Tiger: a fast new hash function. *Lecture Notes in Computer Science*, 1039:89–97, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/link.asp?id=fx0261047446n136; http://www.springerlink.com/openurl.asp?genre=article&id=doi:10.1007/3-540-60865-6_46; http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=1039&spage=89.

Ayadi:1997:VCP

[AB97] M. M. Ayadi and D. Bolignano. Verification of cryptographic protocols: An experiment. *Lecture Notes in Computer Science*, 1313: 358–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

An:1999:CVF

[AB99a] J. H. An and M. Bellare. Constructing VIL-MACs from FIL-MACs: Message authentication under weakened assumptions. In Wiener [Wie99], pages 252–269. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

An:1999:CVM

[AB99b] Jee Hea An and Mihir Bellare. Constructing VIL-MACs from FIL-MACs: Message authentication under weakened assumptions. *Lecture Notes in Computer Science*, 1666: 252–269, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660252.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660252.pdf.

Abadi:1999:STS

[Aba99] Martín Abadi. Secrecy by typing in security protocols. *Journal of the Association for Computing Machinery*, 46(5):749–786, September 1999. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Anderson:1998:NFA

[ABC+98] Ross Anderson, Francesco Bergadano, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas, and Roger Needham. A new family of authentication protocols. *Operating Systems Review*, 32(4):9–20, October 1998. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Ateniese:1996:CBV

[ABDS96] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Constructions and bounds for visual cryptography. *Lecture Notes in Computer Science*, 1099: 416–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Aiello:1998:SAC

[ABDV98] W. Aiello, M. Bellare, G. Di Crescenzo, and R. Venkatesan. Security amplification by composition: The case of doubly-iterated, ideal ciphers. *Lecture Notes in Computer Science*, 1462: 390–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Abe:1998:UVM

[Abe98a] M. Abe. Universally verifiable mix-net with verification work independent of the number of mix-servers. In Nyberg [Nyb98], pages 437–447. ISBN 3-540-64518-7 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1403. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072403.html`.

Abeles:1998:SVP

[Abe98b] Stanley H. Lipson Francine Abeles. Some Victorian periodic polyalphabetic ciphers. In Deavours et al. [DKK+98], pages 309–315. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Abe:1999:RDM

[Abe99] M. Abe. Robust distributed multiplication without interaction. In Wiener [Wie99], pages 130–147.

ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Anderson:1998:SPA

[ABK98a] R. Anderson, E. Biham, and L. Knudsen. Serpent: a proposal for the Advanced Encryption Standard. NIST AES proposal, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, June 1998. ???? pp.

Anderson:1998:SNBa

[ABK98b] Ross Anderson, Eli Biham, and Lars Knudsen. Serpent: a new block cipher proposal. In National Institute of Standards and Technology [Nat98], page ?? ISBN ???? LCCN ???? URL http://www.cl.cam.ac.uk/~rja14/serpent.html. No slides for the conference talk are available.

Anderson:1998:SNBb

[ABK98c] Ross Anderson, Eli Biham, and Lars Knudsen. Serpent: a new block cipher proposal. In Vaudenay [Vau98e], pages 222–238. CODEN LNCSD9. ISBN 3-540-64265-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25F77 1998.

Abadi:1991:ADS

[ABKL91] M. Abadi, M. Burrows, C. Kaufman, and B. Lampson. Authentication and delegation with smartcards. *Lecture Notes in Computer Science*, 526: 326–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Abadi:1993:ADS

[ABKL93] M. Abadi, M. Burrows, C. Kaufman, and B. Lampson. Authentication and delegation with smartcards. *Science of Computer Programming*, 21(2): 93–113, October 1993. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic).

Abadi:1993:CAC

[ABLP93] Martín Abadi, Michael Burrows, Butler Lampson, and Gordon Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, September 1993. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0164-0925/155225.html.

Abraham:1997:SEE

[Abr97] Susan Abraham. Software encryption export policy analysis. Thesis (B.A.), California Polytechnic State University, San

Luis Obispo, CA, USA, 1997. 14 pp.

Auyong:1997:ASC

[AC97] Keok Auyong and Chye-Lin Chee. Authentication services for computer networks and electronic messaging systems. *Operating Systems Review*, 31(3): 3–15, July 1997. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Apolloni:1990:TNN

[ACBR90] B. Apolloni, N. Cesa-Bianchi, and G. Ronchini. Training neural networks to break the knapsack cryptosystem. In *Parallel architectures and neural networks (Salerno, 1990)*, pages 377–382. World Sci. Publishing, Teaneck, NJ, 1990.

ASCFS:1997:XPK

[Acc97] Accredited Standards Committee on Financial Services, X9. X9.30.1-1997, public key cryptography for the financial services industry. American National Standard for Financial Services / part 1, the Digital Signature Algorithm (DSA). Report ANSI X9.30:1-1997, ABA, Washington, DC, USA, January 30, 1997. vii + 18 pp. Revision of X9.30:1-1995.

An:1999:ODR

[ACC99] A. An, N. J. Cercone, and C. Chan. ORTES: The design of a real-time control expert system. *Lecture Notes in Computer Science*, 1609:319–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Angelo:1994:DFS

[ACD94] C. M. Angelo, L. Claesen, and H. De Man. Degrees of formality in shallow embedding hardware description languages in HOL. *Lecture Notes in Computer Science*, 780:87–98, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alexi:1984:RRB

[ACGS84] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr. RSA/Rabin bits are $1/2 + 1\mathrm{Poly}(\log N)$ secure. In IEEE [IEE84], pages 449–457. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.

Alexi:1988:RRF

[ACGS88] Werner Alexi, Benny Z. Chor, Oded Goldreich, and Claus-P. Schnorr. RSA and Rabin functions: Certain parts are as hard as the whole. *SIAM Journal on Computing*, 17(2):194–209, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Acken:1998:HWA

[Ack98] John M. Acken. How watermarking adds value to digital content. *Communications of the Association for Computing Machinery*, 41 (7):75–77, July 1998. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/cacm/1998-41-7/p75-acken/`; `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073101.html`.

ACM:1982:PFA

[ACM82] ACM, editor. *Proceedings of the fourteenth annual ACM Symposium on Theory of Computing, San Francisco, California, May 5–7, 1982*. ACM Press, New York, NY 10036, USA, 1982. ISBN 0-89791-070-2. LCCN QA75.5 .A14 1982. ACM order no. 508820.

ACM:1983:PFA

[ACM83] ACM, editor. *Proceedings of the fifteenth annual ACM Symposium on Theory of Computing, Boston, Massachusetts, April 25–27, 1983*. ACM Press, New York, NY 10036, USA, 1983. ISBN 0-89791-099-0. LCCN QA75.5.A14 1983. ACM order no. 508830.

ACM:1985:PSA

[ACM85] ACM, editor. *Proceedings of the seventeenth annual ACM Symposium on Theory of Computing, Providence, Rhode Island, May 6–8, 1985*. ACM Press, New York, NY 10036, USA, 1985. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6 A13 1985. ACM order no. 508850.

ACM:1986:PEA

[ACM86] ACM, editor. *Proceedings of the Eighteenth annual ACM Symposium on Theory of Computing, Berkeley, California, May 28–30, 1986*. ACM Press, New York, NY 10036, USA, 1986. ISBN 0-89791-193-8. LCCN QA 76.6 A13 1986. ACM order number 508860.

ACM:1987:PNA

[ACM87] ACM, editor. *Proceedings of the nineteenth annual ACM Symposium on Theory of Computing, New York City, May 25–27, 1987*. ACM Press, New York, NY 10036, USA, 1987. ISBN 0-89791-221-7. LCCN QA 76.6 A13 1987.

ACM:1988:PTA

[ACM88] ACM, editor. *Proceedings of the twentieth annual ACM*

Symposium on Theory of Computing, Chicago, Illinois, May 2–4, 1988. ACM Press, New York, NY 10036, USA, 1988. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order no. 508880.

ACM:1989:PEA

[ACM89a] ACM, editor. *Proceedings of the Eighth Annual ACM Symposium on Principles of Distributed Computing: Edmonton, Alberta, Canada, August 14–16, 1989*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-326-4. LCCN QA 76.9 D5 A26 1989.

ACM:1989:PSN

[ACM89b] ACM, editor. *Proceedings, Supercomputing '89: November 13–17, 1989, Reno, Nevada*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-341-8. LCCN QA 76.5 S87 1989. IEEE 89CH2802-7.

ACM:1989:PTF

[ACM89c] *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing: Seattle, Washington, May 15–17, 1989*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989.

ACM:1990:PTS

[ACM90] ACM, editor. *Proceedings of the twenty-second annual ACM Symposium on Theory of Computing, Baltimore, Maryland, May 14–16, 1990*. ACM Press, New York, NY 10036, USA, 1990. ISBN 0-89791-361-2. LCCN QA76.A15 1990. ACM order no. 508900.

ACM:1991:PTT

[ACM91] ACM, editor. *Proceedings of the twenty third annual ACM Symposium on Theory of Computing, New Orleans, Louisiana, May 6–8, 1991*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. ISBN 0-89791-397-3. LCCN QA 76.6 A13 1991. IEEE Computer Society order no. 2190.

ACM:1993:FAC

[ACM93a] ACM, editor. *Fairfax 93: 1st ACM Conference on Computer and Communications Security, 3–5 November 1993, Fairfax, Virginia*. ACM Press, New York, NY 10036, USA, 1993. ISBN 0-89791-629-8. LCCN QA76.9.A25 A26 1993.

ACM:1993:PTF

[ACM93b] ACM, editor. *Proceedings of the twenty-fifth annual ACM Symposium on the Theory of Computing,* *San Diego, California, May 16–18, 1993*. ACM Press, New York, NY 10036, USA, 1993. ISBN 0-89791-591-7. LCCN QA 76.6 A13 1993. ACM order no. 508930.

ACM:1994:AAC

[ACM94a] ACM, editor. *2nd Annual ACM Conference on Computer and Communications Security: November 2–4, 1994, Fairfax, Virginia*. ACM Press, New York, NY 10036, USA, November 1994. ISBN 0-89791-732-4. LCCN QA 76.9 A25 A26 1994. URL http://www.acm.org/pubs/contents/proceedings/commsec/191177.

ACM:1994:CKC

[ACM94b] ACM. Codes, keys, and conflicts: Issues in U.S. crypto policy, June 1994. URL http://info.acm.org/reports/acm_crypto_study.html.

ACM:1994:PTS

[ACM94c] ACM, editor. *Proceedings of the twenty-sixth annual ACM Symposium on the Theory of Computing: Montréal, Québec, Canada, May 23–25, 1994*. ACM Press, New York, NY 10036, USA, 1994. ISBN 0-89791-663-8. LCCN QA76 .A15 1994. ACM order no. 508930.

ACM:1995:PTS

[ACM95] ACM, editor. *Proceedings of the twenty-seventh annual ACM Symposium on Theory of Computing: Las Vegas, Nevada, May 29–June 1, 1995*. ACM Press, New York, NY 10036, USA, 1995. ISBN 0-89791-718-9. LCCN QA 76.6 A13 1995. ACM order no. 508950.

ACM:1996:PAM

[ACM96a] ACM, editor. *Proceedings: ACM Multimedia '96, Boston, Massachusetts, November 18–22, 1996*. ACM Press, New York, NY 10036, USA, 1996. ISBN 0-201-92140-X (Addison Wesley) (??invalid ISBN??), 0-89791-871-1 (ACM). LCCN QA76.575.A36 1996.

ACM:1996:PTE

[ACM96b] ACM, editor. *Proceedings of the twenty-eighth annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, May 22–24, 1996*. ACM Press, New York, NY 10036, USA, 1996. ISBN 0-89791-785-5. LCCN QA 76.6 A13 1996.

ACM:1997:ACC

[ACM97a] ACM, editor. *4th ACM Conference on Computer and Communications Security, Zürich, Switzerland, April 1–4, 1997*. ACM Press, New York,

NY 10036, USA, 1997. ISBN 0-89791-912-2. LCCN ???? URL `http://www.acm.org/pubs/contents/proceedings/commsec/266420/`.

ACM:1997:PEA

[ACM97b] ACM, editor. *Proceedings of the Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, Louisiana, January 5–7, 1997*. ACM Press, New York, NY 10036, USA, 1997. CODEN PAAAF2. ISBN 0-89871-390-0. LCCN ???? URL `http://www.acm.org/pubs/contents/proceedings/soda/314161/`.

ACM:1997:PTN

[ACM97c] ACM, editor. *Proceedings of the twenty-ninth annual ACM Symposium on the Theory of Computing: El Paso, Texas, May 4–6, 1997*. ACM Press, New York, NY 10036, USA, 1997. ISBN 0-89791-888-6. LCCN QA76.5 .A849 1997. ACM order no. 508970.

ACM:1998:AWJ

[ACM98a] ACM, editor. *ACM 1998 Workshop on Java for High-Performance Network Computing, February 28—March 1, 98, Palo Alto, California*. ACM Press, New York, NY 10036, USA, 1998. ISBN ???? LCCN ???? URL `http://www.cs.ucsb.edu/conferences/java98/program.html`.

ACM:1998:PTA

[ACM98b] ACM, editor. *Proceedings of the thirtieth annual ACM Symposium on Theory of Computing: Dallas, Texas, May 23–26, 1998*. ACM Press, New York, NY 10036, USA, 1998. ISBN 0-89791-962-9. LCCN QA75.5 .A14 1998. ACM order number 508980.

ACM:1999:PPA

[ACM99a] ACM, editor. *POPL '99. Proceedings of the 26th ACM SIGPLAN-SIGACT on Principles of programming languages, January 20–22, 1999, San Antonio, TX*, ACM SIGPLAN Notices. ACM Press, New York, NY 10036, USA, 1999. ISBN 1-58113-095-3. LCCN ???? URL `http://www.acm.org/pubs/contents/proceedings/plan/292540/index.html`.

ACM:1999:PTF

[ACM99b] ACM, editor. *Proceedings of the thirty-first annual ACM Symposium on Theory of Computing: Atlanta, Georgia, May 1–4, 1999*. ACM Press, New York, NY 10036, USA, 1999. ISBN 1-58113-067-8. LCCN QA75.5 .A14 1999. ACM order number 508990.

ACM:1999:SPCd

[ACM99c] ACM, editor. *SIGGRAPH 99. Proceedings of the 1999 SIGGRAPH annual conference: Conference abstracts and applications*, Computer Graphics. ACM Press, New York, NY 10036, USA, 1999. ISBN 0-201-48560-5. ISSN 1069-529X. LCCN T385 .S54 1999. URL `http://info.acm.org/pubs/contents/proceedings/graph/`. ACM order number 428990.

Ahlswede:1981:BCG

[AD81] R. Ahlswede and G. Dueck. Bad codes are good ciphers. Report, Universität Bielefeld, Bielefeld, Germany, 1981. Submitted in Nov. 1980 to the proceedings of the International Colloquium on Information Theory, to be held at Budapest in August 1981.

Ajtai:1997:PKC

[AD97] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In ACM [ACM97c], pages 284–293. ISBN 0-89791-888-6. LCCN QA76.5 .A849 1997. URL `http://www.acm.org/pubs/articles/proceedings/stoc/258533/p284-ajtai/p284-ajtai.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/258533/p284-ajtai/`. ACM order no. 508970.

Ajtai:1999:PKC

[AD99] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *STOC '97 (El Paso, TX)*, pages 284–293 (electronic). ACM, New York, 1999.

Adamek:1991:FCT

[Ada91] Jiri Adamek. *Foundations of coding: theory and applications of error-correcting codes, with an introduction to cryptography and information theory*. John Wiley and Sons, Inc., New York, NY, USA, 1991. ISBN 0-471-62187-0. xiii + 336 pp. LCCN QA268 .A36 1991. A Wiley-Interscience publication.

Adam:1992:DSC

[Ada92a] J. A. Adam. Data security — cryptography = privacy? *IEEE Spectrum*, 29(8):29–35, August 1992. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Adams:1992:IAB

[Ada92b] Carlisle M. Adams. On immunity against Biham and Shamir's "differential cryptanalysis". *Information Processing Letters*, 41(2):77–80, February 14, 1992.

CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Adams:1997:CSC

[Ada97a] C. Adams. Constructing symmetric ciphers using the CAST design procedure. *Designs, Codes, and Cryptography*, 12(3): 283–316, 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/jrnltoc.htm/0925-1022. Also available as [Ada97b].

Adams:1997:RCE

[Ada97b] C. Adams. RFC 2144: The CAST-128 encryption algorithm, May 21, 1997. URL ftp://ftp.internic.net/rfc/rfc2144.txt; https://www.math.utah.edu/pub/rfc/rfc2144.txt. See [Ada97a]. Status: INFORMATIONAL.

Adams:1998:CSA

[Ada98] Carlisle Adams. CAST-256: a submission for the Advanced Encryption Standard. In National Institute of Standards and Technology [Nat98], page 33. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf1/cast-slides.pdf. Only the slides for the conference talk are available.

Achour:1999:UUK

[ADBB99] S. Achour, M. Dojat, J.-M. Brethon, and G. Blain. The use of the UMLS knowledge sources for the design of a domain specific ontology: a practical experience in blood transfusion. *Lecture Notes in Computer Science*, 1620:249–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Areces:1999:PRR

[ADD99] C. Areces, H. De Nivelle, and M. De Rijke. Prefixed resolution: a resolution method for modal and description logics. *Lecture Notes in Computer Science*, 1632:187–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Abraham:1991:TSS

[ADDS91] D. G. Abraham, G. M. Dolan, G. P. Double, and J. V. Stevens. Transaction Security System. *IBM Systems Journal*, 30(2): 206–229, 1991. CODEN IBMSA7. ISSN 0018-8670. See erratum [Ano91a].

Appas:1999:SVS

[ADEDS99] A. R. Appas, A. M. Darwish, A. El-Dessouki, and S. I. Shaheen. Speeding the vector search algorithm for regional color channel features based indexing and retrieval systems. *Lecture Notes in Computer Science*, 1611:205–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Augot:1998:DSM

[ADF98] D. Augot, J-F. Delaigle, and C. Fontaine. DHWM: a scheme for managing watermarking keys in the Aquarelle multimedia distributed system. In Quisquater et al. [Q+98], pages 241–255. ISBN 3-540-65004-0. LCCN QA267.A1 L43 no.1485. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073404.html`.

Alagappan:1990:PDA

[ADKN90] K. Alagappan, A. M. De Alvare, D. Klein, and C. Neuman. Panel and discussion on authentication. In USENIX Association [USE90], page ?? LCCN QA 76.9 A25 U55 1990.

Adleman:1979:SAD

[Adl79] L. M. Adleman. A subexponential algorithm for the discrete logarithm. In IEEE [IEE79], pages 55–60. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA267 .S95 1979; TK7885.A1 S92 1979.

Adleman:1983:BGK

[Adl83] Leonard M. Adleman. On breaking generalized knapsack public key cryptosystems. In ACM [ACM83], pages 402–412. ISBN 0-89791-099-0. LCCN QA75.5.A14 1983. ACM order no. 508830.

Adleman:1987:PRD

[Adl87] Leonard Adleman. Pre-RSA days: History and lessons. In Ashenhurst [Ash87], page ?? ISBN 0-201-07794-9. LCCN QA76.24 .A33 1987. ACM Turing Award lecture.

Asokan:1999:APT

[ADSW99] N. Asokan, Hervé Debar, Michael Steiner, and Michael Waidner. Authenticating public terminals. *Computer Networks (Amsterdam, Netherlands: 1999)*, 31(8):861–870, April 23, 1999. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.elsevier.com/cas/tree/store/comnet/sub/1999/31/8/2125.pdf`.

Alves-Foss:1995:ACS

[AFB95] Jim Alves-Foss and Salvador Barbosa. Assessing computer security vulnerability. *Operating Systems Review*, 29(3):3–13, July 1995. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Apostolico:1984:PMM

[AG84] A. Apostolico and R. Giancarlo. Pattern matching machine implementation of a fast test for unique decipherability. *Information Processing Letters*, 18(3): 155–158, March 30, 1984. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Apostolico:1985:CAW

[AG85] Alberto Apostolico and Zvi Galil, editors. *Combinatorial algorithms on words (Maratea, Italy, June 18–22, 1984)*, volume 12 of *NATO Adv. Sci. Inst. Ser. F: Comput. Systems Sci.* Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. ISBN 0-387-15227-X. LCCN QA164 .N35 1984.

Anderson:1995:SFS

[AG95] Scot Anderson and Rick Garvin. Sessioneer: flexible session level authentication with off the shelf servers and clients. *Computer Networks and ISDN Systems*, 27(6):1047–1053, April 3, 1995. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic). URL `http://www.elsevier.com/cas/tree/store/comnet/sub/1995/27/6/1464.pdf`.

Abadi:1997:RAC

[AG97a] M. Abadi and A. D. Gordon. Reasoning about cryptographic protocols in the Spi calculus. *Lecture Notes in Computer Science*, 1243:59–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Abadi:1997:CCPa

[AG97b] Martin Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: the spi calculus. Technical report 414, University of Cambridge Computer Laboratory, Cambridge, UK, January 1997. 105 pp.

Abadi:1997:CCPb

[AG97c] Martin Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: the spi calculus. SRC research report 149, Digital Systems Research Center, ????, January 25, 1997. 110 pp. A preliminary version of this paper appeared as a Technical report of the University of Cambridge Computer Laboratory [AG97b].

Abadi:1998:BMCa

[AG98a] M. Abadi and A. D. Gordon. A bisimulation method for cryptographic protocols. *Lecture Notes in Computer Science*, 1381:12–??, 1998. CODEN LNCSD9. ISSN

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

Abadi:1998:BMCb

[AG98b] Martín Abadi and Andrew D. Gordon. A bisimulation method for cryptographic protocols. *Nordic Journal of Computing*, 5 (4):267–??, Winter 1998. CODEN NJCOFR. ISSN 1236-6064. URL http://www.cs.helsinki.fi/njc/References/abadig1998:267.html.

Aura:1999:SLM

[AG99] Tuomas Aura and Dieter Gollmann. Software license management with Smart Cards. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL http://www.usenix.org/publications/library/proceedings/smartcard99/aura.html.

Agarwal:1992:RSO

[Aga92] Pankaj K. Agarwal. Ray shooting and other applications of spanning trees with low stabbing number. *SIAM Journal on Computing*, 21(3):540–570, June 1992. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Atkins:1995:MWS

[AGLL95] D. Atkins, M. Graff, A. K. Lenstra, and P. C. Leyland. The magic words are squeamish ossifrage. In Pieprzyk and Safavi-Naini [PSN95b], pages 263–277. CODEN LNCSD9. ISBN 3-540-59339-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 1994. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0917.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=917.

Agnew:1987:RSC

[Agn87] G. B. Agnew. Random sources for cryptographic systems. In Chaum and Price [CP87], pages 77–81. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Agnew:1988:RSC

[Agn88] G. B. Agnew. Random sources for cryptographic systems. In Chaum and Price [CP87], pages 77–81. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Afanassiev:1997:FMA

[AGS97] Valentine Afanassiev, Christian Gehrmann, and Ben Smeets. Fast message authentication using efficient polynomial evaluation. *Lecture Notes in Computer Science*, 1267: 190–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670190.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670190.pdf.

Alon:1995:DRV

[AGY95a] N. Alon, Z. Galil, and M. Yung. Dynamic resharing verifiable secret sharing against a mobile adversary. In Spirakis [Spi95], pages 523–537. CODEN LNCSD9. ISBN 3-540-60313-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A43 E83 1995.

Alou:1995:EDR

[AGY95b] N. Alou, Z. Galil, and M. Yung. Efficient dynamic-resharing "verifiable secret sharing" against mobile adversary. *Lecture Notes in Computer Science*, 979: 523–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alberda:1997:UFM

[AHdJF97] Marjan I. Alberda, Pieter H. Hartel, and Eduard K. de Jong Frz. Using formal methods to cultivate trust in smart card operating systems. *Future Generation Computer Systems*, 13(1): 39–54, June 20, 1997. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.elsevier.com/gej-ng/10/19/19/28/17/19/abstract.html.

Autexier:1999:SDI

[AHMS99] S. Autexier, D. Hutter, H. Mantel, and A. Schairer. System description: inka 5.0 — a logic voyager. *Lecture Notes in Computer Science*, 1632:207–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Aiello:1998:NCS

[AHV98] William Aiello, Stuart Haber, and Ramarathnam Venkatesan. New constructions for secure hash functions. *Lecture Notes in Computer Science*, 1372: 150–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720150.htm; http://link.springer-ny.com/link/service/series/0558/papers/1372/13720150.pdf.

Akritas:1983:CEA

[AIR83] A. G. Akritas, S. S. Iyengar,

and A. A. Rampuria. Computationally efficient algorithms for a one-time pad scheme. *International Journal of Computer and Information Sciences*, 12(4):285–316, August 1983. CODEN IJCIAH. ISSN 0091-7036.

Angluin:1995:WWM

[AK95] Dana Angluin and Michael Kharitonov. When won't membership queries help? *Journal of Computer and System Sciences*, 50(2):336–355, 1995. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). 23rd Symposium on the Theory of Computing (New Orleans, LA, 1991).

Al-Kadi:1998:OCA

[AK98] Ibrahim A. Al-Kadi. Origins of cryptology: the Arab contribution. In Deavours et al. [DKK+98], pages 93–122. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Alvarez:1999:AAS

[AK99] David Alvarez and David Kahn, editors. *Allied and Axis Signals Intelligence in World War II*. Cass series–studies in intelligence. Frank Cass Publishers, Portland, OR, 1999. ISBN 0-7146-4958-9, 0-7146-8019-2 (paperback). ISSN 1368-9916. 229 pp. LCCN D810.C88 A45 1999. UK£37.50.

Aberer:1994:DUO

[AKF94] K. Aberer, W. Klas, and A. L. Furtado. Designing a user-oriented query modification facility in object-oriented database systems. *Lecture Notes in Computer Science*, 811:380–393, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Akoka:1999:CDP

[Ako99] J. Akoka. Conceptual design of parallel systems. *Lecture Notes in Computer Science*, 1565:1–23, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Abdelguerfi:1996:GEI

[AKP96] Mahdi Abdelguerfi, Burton S. Kaliski, Jr., and Wayne Patterson. Guest Editors' introduction: Public-key security systems. *IEEE Micro*, 16(3):10–13, May/June 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Anlauff:1999:TSL

[AKP99] M. Anlauff, P. W. Kutter, and A. Pierantonio. Tool support for language design and prototyping with montages. *Lecture Notes in Computer Science*, 1575: 296–300, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

AlJabri:1996:UDU

[Al 96] A. Kh. Al Jabri. The unicity distance: an upper bound on the probability of an eavesdropper successfully estimating the secret key. *Information Processing Letters*, 60(1):43–47, October 14, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Alabbadi:1993:IEC

[Ala93a] Mohssen Alabbadi. *Integration of error correction, encryption, and signature based on linear error-correcting block codes*. Thesis (Ph.D.), School of Electrical Engineering, Georgia Institute of Technology, Atlanta, GA, USA, 1993. xii + 185 pp. Directed by Stephen B. Wicker.

Alagappan:1993:RTA

[Ala93b] K. Alagappan. RFC 1412: Telnet Authentication: SPX, January 1993. URL `ftp://ftp.internic.net/rfc/rfc1412.txt; https://www.math.utah.edu/pub/rfc/rfc1412.txt`. Status: EXPERIMENTAL.

Alabbadi:1997:SCH

[Ala97] M. M. Alabbadi. Security comments on the Hwang–Chen algebraic-code cryptosystem. *Lecture Notes in Computer Science*, 1334: 274–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alberti:1470:TC

[Alb70] Leon Battista Alberti. *Trattati in Cifra. (Italian) [Treatises in ciphers]*. ????, ????, 1470. ???? pp.

Alexander:1945:CHG

[Ale45] C. H. O'D. Alexander. Cryptologic history of the German Naval Enigma. GC&CS Report HW 25/7, British National Archives, ????, 1945.

Alexandris:1992:FMC

[Ale92] N. Alexandris. Factorization methods in cryptosystems. *Bull. Greek Math. Soc.*, 34:65–82, 1992. ISSN 0072-7466.

Alexandre:1997:BSC

[Ale97] Thomas J. Alexandre. Biometrics on smart cards: an approach to keyboard behavioral signature. *Future Generation Computer Systems*, 13(1):19–26, June 20, 1997. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.elsevier.com/gej-ng/10/19/19/28/17/18/abstract.html.

Alexandre:1998:JBP

[Ale98] Thomas J. Alexandre. A Java-based platform for intellectual property protection on the World Wide Web. *Computer Networks and ISDN Systems*, 30(1–7):591–593, April 1, 1998. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072101.html; http://www.elsevier.com/cas/tree/store/comnet/sub/1998/30/1-7/1863.pdf.

Allen:1997:DEC

[All97] Heber E. Allen. Data encryption and conflict with free speech. Thesis (Bachelor's), Arizona State University, Tempe, AZ, USA, 1997. 31 pp.

Allen:1998:SUM

[All98] Chaka Allen. Steganography using the minimax eigenvalue decomposition. Thesis (M.S.), Iowa State University, Ames, IA, USA, 1998. 46 pp.

Ahituv:1987:PED

[ALN87a] Niv Ahituv, Yeheskel Lapid, and Seev Neumann. Processing encrypted data. *Communications of the Association for Computing Machinery*, 30(9):777–780, September 1987. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/30404.html.

Ahituv:1987:VAI

[ALN87b] Niv Ahituv, Yeheskel Lapid, and Seev Neumann. Verifying the authentication of an information system user. *Computers and Security*, 6(2):152–157, April 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900861.

Aiello:1998:FDI

[ALO98] W. Aiello, S. Lodha, and R. Ostrovsky. Fast digital identity revocation. *Lecture Notes in Computer Science*, 1462:137–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alvarez:1998:FLV

[Alv98a] David Alvarez. Faded lustre: Vatican cryptography, 1815–1920. In Deavours et al. [DKK+98], pages 191–225. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://

www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Alvarez:1998:IDC

[Alv98b] David Alvarez. Italian diplomatic cryptanalysis in World War I. In Deavours et al. [DKK+98], pages 181–190. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Alvarez:1998:PCS

[Alv98c] David Alvarez. The Papal Cipher Section in the early Nineteenth Century. In Deavours et al. [DKK+98], pages 155–160. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Akl:1985:FPR

[AM85] Selim G. Akl and Henk Meijer. A fast pseudo random permutation generator with applications to cryptology. In Blakley and Chaum [BC85], pages 269–275. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=269. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Adams:1988:SRC

[AM88] Carlisle M. Adams and Henk Meijer. Security-related comments regarding McEliece's public-key cryptosystem. *Lecture Notes in Computer Science*, 293: 224–228, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Adams:1989:SRC

[AM89] Carlisle M. Adams and Henk Meijer. Security-related comments regarding McEliece's public-key cryptosystem. *IEEE Transactions on Information Theory*, IT-35(2):454–455, 1989. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Anderson:1997:CNK

[AM97] R. Anderson and C. Manifavas. Chameleon — a new kind of stream cipher. *Lecture Notes in Computer Science*, 1267:107–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Atanasiu:1999:ASE

[AM99] Adrian Atanasiu and Victor Mitrana. About symbolic encryption: separable encryption systems. In *Grammatical models of multi-agent systems*, volume 8 of *Topics in Comput. Math.*, pages 219–225. Gordon and Breach, Amsterdam, 1999.

ACE:1981:RPC

[Ame81] American Council on Education. Report of the Public Cryptography Study Group. *Communications of the Association for Computing Machinery*, 24(7): 435–450, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See the opposing view in [Dav81].

ANSI:1983:ANS

[Ame83] American National Standards Institute. *American National Standard for information systems: data encryption algorithm: modes of operation*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, 1983. ?? pp.

ABAECITC:1995:DSG

[Ame95] American Bar Association.Electronic Commerce and Information and Technology Division. *Digital signature guidelines: legal infrastructure for certification authorities and electronic commerce: draft October 5, 1995*. American Bar Association, Chicago, IL, USA, 1995. viii + 100 pp.

ABAECITDISC:1996:DSG

[Ame96a] American Bar Association.Electronic Commerce and Information and Technology Division. Information Security Committee. *Digital signature guidelines: legal infrastructure for certification authorities and electronic commerce*. American Bar Association, Chicago, IL, USA, August 1, 1996. ISBN 1-57073-250-7. v + 99 pp. LCCN KF810.D44 1996.

Ames:1996:SDM

[Ame96b] M. Ames. Saving dollars makes sense of crypto export controls. *Lecture Notes in Computer Science*, 1029:90–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anton:1994:GDS

[AMP94] A. I. Anton, W. M. McCracken, and C. Potts. Goal decomposition and scenario analysis in business process reengineering. *Lecture Notes in Computer Science*, 811:94–104, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Arnal:1999:SAP

[AMP99] J. Arnal, V. Migallon, and J. Penades. Synchronous and asynchronous parallel algorithms with overlap for almost linear systems. *Lecture Notes in Computer Science*, 1573:142–155, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anderson:1996:NPE

[AMS96] R. Anderson, H. Manifavas, and C. Sutherland. NetCard — a practical electronic cash systems, 1996. URL mailto:Ross.Anderson@cl.cam.ac.uk.

Agnew:1990:FEC

[AMV90] Gordon B. Agnew, R. C. Mullin, and Scott A. Vanstone. A fast elliptic curve cryptosystem. *Lecture Notes in Computer Science*, 434:706–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340706.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340706.pdf.

Agnew:1993:DFE

[AMV93] Gordon B. Agnew, R. C. Mullin, and Scott A. Vanstone. On the development of a fast elliptic curve cryptosystem. *Lecture Notes in Computer Science*, 658:482–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580482.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580482.pdf.

Andrew:1986:TCB

[AN86] Christopher Andrew and Keith Neilson. Tsarist codebreakers and British codes. *Intelligence and National Security*, 1(1):6–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Abadi:1994:PEP

[AN94] Martin Abadi and R. M. Needham. Prudent engineering practice for cryptographic protocols. Technical report, Digital Systems Research Center, ????, June 1, 1994. 25 pp. A preliminary version of this paper has appeared in the Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy.

Anderson:1995:RPP

[AN95] Ross Anderson and Roger Needham. Robustness principles for public key protocols. *Lecture Notes in Computer Science*, 963: 236–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630236.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0963/09630236.pdf`.

Abadi:1996:PEP

[AN96] M. Abadi and R. Needham. Prudent engineering practice for cryptographic protocols. *IEEE Transactions on Software Engineering*, 22(1):6–15, January 1996. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=481513`.

Andree:1952:C

[And52] Richard Vernon Andree. *Cryptanalysis*. Yeshiva College, New York, NY, USA, 1952. 5–16 pp. Reprinted from Scripta mathematica, Vol. 28, No. 1. March, 1952.

Andelman:1979:MLE

[And79] Dov Andelman. *Maximum likelihood estimation applied to cryptanalysis*. Thesis (Ph.D.), Stanford University, Stanford, CA, USA, 1979. viii + 167 pp.

Andelman:1980:MLE

[And80] Dov Andelman. *Maximum likelihood estimation applied to cryptanalysis*. Thesis (Ph.D.), Department of Electrical Engineering, Stanford University, Stanford, CA, USA, 1980. viii + 167 pp.

Andrew:1986:CSI

[And86] Christopher Andrew. Codebreaking and signals intelligence. *Intelligence and National Security*, 1(1):1–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Anderson:1993:PRT

[And93] R. J. Anderson. A practical RSA trapdoor. *Electronic Letters*, ??(??):29–??, ???? 1993. URL `????`.

Anderson:1994:FSE

[And94a] Ross Anderson, editor. *Fast software encryption: Cambridge Security Workshop, Cambridge, UK, December 9–11, 1993: proceed-*

ings, volume 809 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 3-540-58108-1, 0-387-58108-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C36 1993.

Anderson:1994:WCF

[And94b] Ross J. Anderson. Why cryptosystems fail. *Communications of the Association for Computing Machinery*, 37(11):32–40, November 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/188291.html`.

Anderson:1996:CEM

[And96a] R. Anderson. Crypto in Europe — markets, law and policy. *Lecture Notes in Computer Science*, 1029: 75–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anderson:1996:SLS

[And96b] R. Anderson. Stretching the limits of steganography. *Lecture Notes in Computer Science*, 1174:39–48, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054101.html`.

Anderson:1996:IHF

[And96c] Ross Anderson, editor. *Information hiding: first international workshop, Cambridge, U.K., May 30–June 1, 1996: proceedings*, volume 1174 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996.

Anderson:1998:EWF

[And98] Steven P. Anderson. Encryption and watermark the future of copyright?, 1998. 1 sound cassette.

Anonymous:1922:PUS

[Ano22] Anonymous. Practical uses for the spectroscope, secret radio communication. *Scientific American*, 127(4): 259, October 1922. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v127/n4/pdf/scientificamerican1022-259.pdf`.

Anonymous:1939:ITM

[Ano39] Anonymous. Introductory talk to members of the William and Mary College cryptanalysis class. Technical report, William and Mary College, Williamsburg, VA, USA, 1939. 7 pp.

Anonymous:1960:CNH

[Ano60] Anonymous. *Cryptanalysis, a new horizon, by Dr. Cryptogram [pseudonym]*. American Cryptogram Association, New York, NY, USA (??), 1960. 10 + 1 + 27 pp.

Anonymous:1976:CCA

[Ano76] Anonymous. *Cryptography and cryptanalysis articles*, volume 5 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-003-4. v + 144 pp. LCCN ????

Anonymous:1978:CSD

[Ano78a] Anonymous, editor. *Computer security and the Data Encryption Standard: proceedings of the Conference on Computer Security and the Data Encryption Standard held at the National Bureau of Standards in Gaithersburg, Maryland, on February 15, 1977*, volume 500-27 of *NBS special publication, computer science and technology*. United States Government Printing Office, Washington, DC, USA, 1978.

Anonymous:1978:NPAd

[Ano78b] Anonymous. New product applications: Single-board bipolar microcomputer emulates any mini- or microcomputer. *IEEE Spectrum*, 15(4):68–73, April 1978. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:1978:ODA

[Ano78c] Anonymous. *The origin and development of the Army Security Agency, 1917–1947*, volume 16 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1978. ISBN 0-89412-025-5. 51 pp. LCCN UB290 .O75 1978.

Anonymous:1979:SSA

[Ano79] Anonymous. SB. Security Agency denies tampering with DES. *IEEE Spectrum*, 16(7):39, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:1980:ACS

[Ano80] Anonymous. An assessment of civil sector uses of digital data encryption. Technical report, Department of Engineering and Public Policy, Department of Social Sciences and School of Urban and Public Affairs, Carnegie-Mellon University, Pittsburgh, PA, USA, November 1980. 128 pp.

Anonymous:1981:CHP

[Ano81a] Anonymous. Corrections: How Polish Mathematicians Deciphered the Enigma, 3(3) 232, Reviews: H. H. Goldstine: A History of Numerical Analysis, 3(3) 293. *Annals of the History of Computing*, 3(4):407, October/December 1981. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1981/pdf/a4400.pdf. See [Rej81, SWT+81].

Anonymous:1981:GIU

[Ano81b] Anonymous. *Guidelines for implementing and using the NBS Data Encryption Standard*, volume 74 of *United States. National Bureau of Standards. Federal information processing standards publication, FIPS PUB*. U.S. National Bureau of Standards, Gaithersburg, MD, USA, 1981. ISSN 0083-1816. 39 pp.

Anonymous:1982:BRCa

[Ano82a] Anonymous. Book review: *Cryptography: a primer*: Alan G. Konheim: New York: John Wiley and Sons, 1981. xiv + 432 pp. $34.95. *Computers and Security*, 1(1):84, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488290030X.

Anonymous:1982:CC

[Ano82b] Anonymous. *A course in cryptanalysis*, volume 33, 34 of *Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1982. ISBN 0-89412-052-2 (vol. 1), 0-89412-053-0 (vol. 2). LCCN ????

Anonymous:1982:ESS

[Ano82c] Anonymous. Encryption scrambling the satellite signal for security, 1982. 1 sound cassette (75 min.).

Anonymous:1982:NNPa

[Ano82d] Anonymous. News and notices: Pioneer Award Established by Computer Society; Undergraduate Paper Competition in Cryptology. *Annals of the History of Computing*, 4(2):184, April/June 1982. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1982/pdf/a2184.pdf; http://www.computer.org/annals/an1982/a2184abs.htm.

Anonymous:1984:BRP

[Ano84a] Anonymous. Book review: *The puzzle palace: a report on NSA, America's most* *secret agency*: James Bamford: Boston: Houghton Mifflin Company, 1982, 465 pages. $16.95. *Computers and Security*, 3(1):57, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900300`.

Anonymous:1984:ESC

[Ano84b] Anonymous. *EDP security: communications, database, end user, encryption: advanced security concepts*. Number 3 in FTP technical library EDP security. FTP, Port Jefferson Station, NY, USA, 1984. various pp.

Anonymous:1985:BM

[Ano85a] Anonymous. Back matter. In Blakley and Chaum [BC85], page ?? CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=??`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Anonymous:1985:DEA

[Ano85b] Anonymous. Data encryption algorithm: Electronic funds transfer: requirements for interfaces. Technical report, ????, ????, 1985. ISBN 0-7262-3764-7. 16 pp.

Anonymous:1986:MTT

[Ano86a] Anonymous. Modern technology tools for user authentication. *Computers and Security*, 5(3):184–185, September 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886900039`.

Anonymous:1986:CPC

[Ano86b] Anonymous. On cryptographic protection of capabilities. *Computers and Security*, 5(2):98–99, June 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886901306`.

Anonymous:1986:RE

[Ano86c] Anonymous. Remember the Enigma! *Computers and Security*, 5(4):288–289, December 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404886900489.

Anonymous:1987:EVE

[Ano87a] Anonymous. *Enigma variations: encryption, emc/rfi, emp: 1987 conference proceedings*. Osprey Exhibitions, Watford, England, 1987. v + 243 pp.

Anonymous:1987:HSE

[Ano87b] Anonymous. High-speed encrypted storage/backup. *Computers and Security*, 6(5):370–373, October 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900034.

Anonymous:1987:MAU

[Ano87c] Anonymous. Message authentication using the RSA. *Computers and Security*, 6(5):373–376, October 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900046.

Anonymous:1987:TWP

[Ano87d] Anonymous. Technology watch — personal authentication devices. *Computers and Security*, 6(1):10–11, February 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887901143.

Anonymous:1988:BRCb

[Ano88a] Anonymous. Book review: *Computer viruses — a secret threat*: Rudiger Dierstein. *Computers and Security*, 7(2):215, April 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888903537.

Anonymous:1988:CCJc

[Ano88b] Anonymous. Cryptography and cryptosystems. January 1970–October 1987. *Computers and Security*, 7(5):519, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888902738.

Anonymous:1988:CCJb

[Ano88c] Anonymous. Cryptography and cryptosystems. January 1987–December 1987 (citations from the INSPEC: Information Services for the Physics and Engineering Communities database). *Computers and Security*, 7(5):518, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https:/

/www.sciencedirect.com/science/article/pii/0167404888902593.

Anonymous:1988:DEK

[Ano88d] Anonymous. Data encryption is key to safe file transmission: *Lawrence E. Hughes*. *Computers and Security*, 7(2): 221, April 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888903926.

Anonymous:1988:DESb

[Ano88e] Anonymous. Data encryption standard. 1975–January 1987 (citations from the INSPEC: Information Services for the Physics and Engineering Communities database). *Computers and Security*, 7(5):511, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888902155.

Anonymous:1988:DESa

[Ano88f] Anonymous. Data Encryption Standard. January 1975–January 1988 (citations from the INSPEC: Information Services for the Physics and Engineering Communications Database). *Computers and Security*, 7(5):511, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888902143.

Anonymous:1988:EVE

[Ano88g] Anonymous, editor. *Enigma variations: encryption, EMC/RFI, EMP: 1988 conference proceedings*. Osprey Exhibitions, Watford, England, 1988.

Anonymous:1988:ERH

[Ano88h] Anonymous. Errata: Reviews: Hartree: Calculating Machines: Recent and Prospective Developments and Their Impact on Mathematical Physics and Calculating Instruments and Machines, 10(1) 93. *Annals of the History of Computing*, 10(3):234, July/September 1988. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1988/pdf/a3234.pdf; http://www.computer.org/annals/an1988/a3234abs.htm. See [AWL+88].

Anonymous:1988:PED

[Ano88i] Anonymous. Processing encrypted data: Niv Ahituv, Yeheskel Lapid, and Seev Neumann. *Computers and Security*, 7(1):103, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488890524X.

Anonymous:1988:RIA

[Ano88j] Anonymous. Remote identification and authentication of computer resource users: *Ken Weiss*. *Computers and Security*, 7(2): 214, April 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888903495.

Anonymous:1989:SZS

[Ano89] Anonymous. The safety zone (security products for microcomputers). *BYTE Magazine*, 14(6):290–291, June 1989. CODEN BYTEDJ. ISSN 0360-5280.

Anonymous:1990:SEL

[Ano90] Anonymous. A standard for extremely low frequency magnetic fields; standards for public key encryption algorithms to be discussed. *Computer*, 23(4): 95–??, April 1990. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Anonymous:1991:ESS

[Ano91a] Anonymous. Erratum: "Transaction Security System". *IBM Systems Journal*, 30(4):598, 1991. CODEN IBMSA7. ISSN 0018-8670. See [ADDS91].

Anonymous:1991:FFL

[Ano91b] Anonymous. Fax facts: The little-known digital secrets tucked inside every fax device. *BYTE Magazine*, 16 (2):301–??, February 1991. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1991:E

[Ano91c] Anonymous. On the Enigma. *Cryptolog*, 18 (2):31–32, 1991. ISSN 0740-7602. URL https://archive.org/download/cryptolog_121/cryptolog_121.pdf.

Anonymous:1992:AUd

[Ano92a] Anonymous. Answers to UNIX. *UNIX/world*, 9(9): 121–??, September 1992. ISSN 0739-5922.

Anonymous:1992:DES

[Ano92b] Anonymous. Debating encryption standards. *Communications of the Association for Computing Machinery*, 35(7):32–34, July 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/129903.html.

Anonymous:1992:DDS

[Ano92c] Anonymous. Double data security. *Datamation*, 38 (??):21–??, November 15,

1992. CODEN DTMNAT. ISSN 0011-6963.

Anonymous:1993:ACT

[Ano93a] Anonymous. Anti-counterfeit trials begin with watermark technology. *Financial Technology International Bulletin*, XI(2):6–7, October 1993. CODEN FTIBFY. ISSN 0265-1661. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/024122.html.

Anonymous:1993:BRd

[Ano93b] Anonymous. Book reviews. *Scientific American*, 268(4): 123–??, April 1993. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Anonymous:1993:CKR

[Ano93c] Anonymous. Can Kerberos really make UNIX secure? *Datamation*, 39(1): 59–??, January 01, 1993. CODEN DTMNAT. ISSN 0011-6963.

Anonymous:1993:CSA

[Ano93d] Anonymous, editor. *Computer security, audit and control: 10th World conference — October 1993, London*, PROCEEDINGS OF COMPSEC INTERNATIONAL 1993; 10th. Elsevier Advanced Technology, Oxford, UK, 1993. ISBN 1-85617-211-2. LCCN ????

Anonymous:1993:CNh

[Ano93e] Anonymous. CS news. *Computer*, 26(11):76–??, November 1993. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Anonymous:1993:FSH

[Ano93f] Anonymous. *FIPS 180, Secure Hash Standard*. NIST, US Department of Commerce, Washington, DC, USA, May 1993.

Anonymous:1993:JIK

[Ano93g] Anonymous, editor. *JW-ISC 93: Korea-Japan Joint Workshop on Information Security and Cryptology, Seoul, Korea, 24–26 October 1993*. ????, ????, 1993. ISBN ???? LCCN ????

Anonymous:1993:LC

[Ano93h] Anonymous, editor. *Laser Communications 93*. ????, ????, 1993. ISBN ???? LCCN ????

Anonymous:1993:SBh

[Ano93i] Anonymous. Science and business. *Scientific American*, 269(2):112–??, August 1993. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Anonymous:1993:SMC

[Ano93j] Anonymous. Secure E-Mail Cheaply With Software Encryption. *Datamation*, 39 (23):48–??, December 01,

1993. CODEN DTMNAT. ISSN 0011-6963.

Anonymous:1993:WND

[Ano93k] Anonymous. What's new: The DTR-1 is a notebook or a pen computer, the SmartLink V32bis FaxModem encrypts your data, LapCAD 5 for the Mac gives you finite modeling, and more. *BYTE Magazine*, 18 (6):57–??, May 1993. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1994:CNc

[Ano94a] Anonymous. CS news. *Computer*, 27(4):63–??, April 1994. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Anonymous:1994:DAX

[Ano94b] Anonymous. *Draft ANSI X9.44 RSA Key Transport Standard*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, October 1994. ?? pp.

Anonymous:1994:ERB

[Ano94c] Anonymous. Encryption restrictions bind manufacturer's hands. *Network Security*, 1994(6): 6, June 1994. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/1353485894900388`.

Anonymous:1994:HSK

[Ano94d] Anonymous. Highway safety: The key is encryption. *BYTE Magazine*, 19(3):60–??, March 1994. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1994:ICI

[Ano94e] Anonymous, editor. *ICIP-94: proceedings, November 13–16, 1994, Austin Convention Center, Austin, Texas*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-6951-9 (microfiche). LCCN TA 1637 I25 1994. Three volumes. IEEE Computer Society Press Order Number 6950-02. IEEE catalog number 94CH35708.

Anonymous:1994:KEE

[Ano94f] Anonymous. *Key escrow encryption: announcements — February 4, 1994*. ????, ????, 1994. various pp.

Anonymous:1994:Lba

[Ano94g] Anonymous. LANScape. *Datamation*, 40(20):38–??, October 15, 1994. CODEN DTMNAT. ISSN 0011-6963.

Anonymous:1994:Ll

[Ano94h] Anonymous. LANScape. *Datamation*, 40(20):38–??, October 15, 1994. CODEN DTMNAT. ISSN 0011-6963.

Anonymous:1994:PRP

[Ano94i] Anonymous. Product review: Pretty Good Privacy is a privacy advocate's plan to head off the government's bid to snoop on data. *Open Systems Today*, 162:56–??, October 1994. ISSN 1061-0839.

Anonymous:1994:Uc

[Ano94j] Anonymous. Update. *Computer*, 27(6):78–??, June 1994. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Anonymous:1994:WAS

[Ano94k] Anonymous. Whose authentication systems? *BYTE Magazine*, 19(10):128–??, October 1994. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1995:AUC

[Ano95a] Anonymous. Algorithms update: Collisions in MD4; more developments with keyed hash functions; A linear protocol failure for RSA with exponent three. *CryptoBytes*, 1(3):4–6, Autumn 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf`.

Anonymous:1995:AUM

[Ano95b] Anonymous. Algorithms update: MD5 performance for IP security questioned. *CryptoBytes*, 1(2):13–14, Summer 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf`.

Anonymous:1995:EES

[Ano95c] Anonymous. An E-mail encryption standard should be in place by April, providing for the incorporation of Privacy Enhanced Mail into the MIME standard. *Open Systems Today*, 168:26–??, February 1995. ISSN 1061-0839.

Anonymous:1995:ARLa

[Ano95d] Anonymous. Announcements: 1995 RSA Laboratories seminar series. *CryptoBytes*, 1(1):12, Spring 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n1.pdf`.

Anonymous:1995:ARLb

[Ano95e] Anonymous. Announcements: RSA Laboratories technical reports. *CryptoBytes*, 1(2):15, Summer 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf`.

Anonymous:1995:ARD

[Ano95f] Anonymous. Announcements: The 1996 RSA Data Security Conference. *CryptoBytes*, 1(3): 16, Autumn 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf.

Anonymous:1995:DAS

[Ano95g] Anonymous. Defender authentication software. *Network Security*, 1995(4): 6, April 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485895902228.

Anonymous:1995:ENa

[Ano95h] Anonymous. Editor's note. *CryptoBytes*, 1(2): 2, Summer 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf.

Anonymous:1995:ENb

[Ano95i] Anonymous. Editor's note. *CryptoBytes*, 1(3): 2, Autumn 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf.

Anonymous:1995:EEW

[Ano95j] Anonymous. Europe encrypts weather data. *Network Security*, 1995(6): 5, June 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485896897169.

Anonymous:1995:ENE

[Ano95k] Anonymous. Europe negotiates over encryption. *Network Security*, 1995(8): 4, August 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485895900861.

Anonymous:1995:FSH

[Ano95l] Anonymous. *FIPS 180-1, Secure Hash Standard*. National Institute of Standards and Technology, US Department of Commerce, Washington, DC, USA, April 1995. ?? pp.

Anonymous:1995:FRE

[Ano95m] Anonymous. Frame relay encryptor protects. *Network Security*, 1995(10):5–6, October 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485895902694.

Anonymous:1995:HPE

[Ano95n] Anonymous. H-P's encryption engine proposal. *Network Security*, 1995(10):6, October 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485896897534.

Anonymous:1995:IUA

[Ano95o] Anonymous. Internet user authentication security. *Network Security*, 1995 (11):5, November 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485895901531.

Anonymous:1995:NIX

[Ano95p] Anonymous. News and information: X9F1 considers triple-DES standard; RSA Laboratories publishes PKCS #11. *CryptoBytes*, 1 (1):11, Spring 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n1.pdf.

Anonymous:1995:OIN

[Ano95q] Anonymous. Oracle is now shipping encryption software for securing data on SQL*Net 2.1 networks — even data going to non-Oracle databases. *Open Systems Today*, 167:29–??, January 1995. ISSN 1061-0839.

Anonymous:1995:PTN

[Ano95r] Anonymous, editor. *Proceedings of the Twenty-Ninth Annual Conference on Information Sciences and Systems: papers presented March 22, 23, and 24, 1995*, volume 29 of *Proceedings of the Conference on Information Sciences and Systems*. The John Hopkins University, Baltimore, MD, 1995. LCCN ????

Anonymous:1995:RLM

[Ano95s] Anonymous. RSA Laboratories minimum key size recommendations. *CryptoBytes*, 1(2):12, Summer 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf.

Anonymous:1995:SDE

[Ano95t] Anonymous. SentryLink data encryption devices. *Network Security*, 1995(4): 5, April 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485895902201.

Anonymous:1995:SUE

[Ano95u] Anonymous. Standards update: Elliptic curves in Draft IEEE Standard; S/MIME standardized. *CryptoBytes*, 1(2):4, Summer 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf.

Anonymous:1995:SEE

[Ano95v] Anonymous. Stronger encryption exportable. *Network Security*, 1995(8):3, August 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485895900845.

Anonymous:1995:TEV

[Ano95w] Anonymous. Telnet encryption vulnerability. *Network Security*, 1995(2):2, February 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485895901132.

Anonymous:1995:XAV

[Ano95x] Anonymous. X authentication vulnerability. *Network Security*, 1995(12):2, December 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485895901566.

Anonymous:1996:NIS

[Ano96a] Anonymous, editor. *19th National Information Systems Security Conference, October 22–25, 1996, Baltimore Convention Center, Baltimore, Maryland*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 1996. LCCN QA76.9.A25 N36 1996.

Anonymous:1996:RF

[Ano96b] Anonymous. Algorithms update: RSA-130 factored. *CryptoBytes*, 2(2): 7, Summer 1996. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n2.pdf.

Anonymous:1996:ADX

[Ano96c] Anonymous. *ANSI draft X9.52, Triple Data Encryption Algorithm Modes of Operation, Revision 6.0*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, May 1996. ?? pp.

Anonymous:1996:BCU

[Ano96d] Anonymous. Before the court unauthorized encryption: a CFP moot court, 1996. ISBN 1-57844-030-0. 1 videocassette (120 min.).

Anonymous:1996:CED

[Ano96e] Anonymous. Compress and encrypt data simultaneously. *Network Security*, 1996(2):4–5, February 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896900471.

Anonymous:1996:CID

[Ano96f] Anonymous. Correction to “Improved Digital Signature Algorithm”. *IEEE*

Transactions on Computers, 45(7):864, July 1996. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=508326. See [YL95b].

Anonymous:1996:CCC

[Ano96g] Anonymous. Credit-card company seeks strong encryption. *Network Security*, 1996(7):5, July 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896900975.

Anonymous:1996:CSIa

[Ano96h] Anonymous. Crypto system initialization: Simplifying the distribution of initial keys: Carl Meyer, IBM. *Computers and Security*, 15 (5):406, ???? 1996. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404896826034.

Anonymous:1996:CPD

[Ano96i] Anonymous. Cryptographic policy debate. *IEEE Software*, 13(2):116, March 1996. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Anonymous:1996:CPT

[Ano96j] Anonymous. CryptoSystem protects TCP/IP networks. *Network Security*, 1996(8): 4–5, August 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896900392.

Anonymous:1996:ENa

[Ano96k] Anonymous. Editor's note. *CryptoBytes*, 2(1): 2, Spring 1996. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n1.pdf.

Anonymous:1996:ENb

[Ano96l] Anonymous. Editor's note. *CryptoBytes*, 2(2): 2, Summer 1996. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n2.pdf.

Anonymous:1996:EME

[Ano96m] Anonymous. Electronic mail encryption standards' rivalry. *Network Security*, 1996(6):3, June 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901373.

Anonymous:1996:EBS

[Ano96n] Anonymous. Encryption battle sees possible break through. *Network Security*, 1996(5):2, May 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901063.

Anonymous:1996:ERK

[Ano96o] Anonymous. Encryption report kept under lock and key. *Network Security*, 1996 (1):3, January 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901543.

Anonymous:1996:ERM

[Ano96p] Anonymous. Encryption restrictions may be eased. *Network Security*, 1996(4): 2–3, April 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901750.

Anonymous:1996:EKE

[Ano96q] Anonymous. Encryption without key exchange. *Network Security*, 1996(9):4–5, September 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896900264.

Anonymous:1996:ECC

[Ano96r] Anonymous. The EPS CD and CD-ROM security conference 1995. *The Computer Law and Security Report*, 12(1): 28–36, January/February 1996. CODEN CLSRE8. ISSN 0267-3649. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/051315.html.

Anonymous:1996:FDC

[Ano96s] Anonymous. Fundamental DES design concepts: Carl Meyer, IBM. *Computers and Security*, 15(5): 406, ???? 1996. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404896826022.

Anonymous:1996:GPT

[Ano96t] Anonymous. Governments pressed Tor agreement on encryption. *Network Security*, 1996(3):3, March 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901191.

Anonymous:1996:HET

[Ano96u] Anonymous. Hardware encryption technology complies with encryption regulations. *Network Security*, 1996(12):4, December 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896900768.

Anonymous:1996:LAW

[Ano96v] Anonymous. On-LAN authentication for Windows NT. *Network Security*, 1996 (9):4, September 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896900252.

Anonymous:1996:PKE

[Ano96w] Anonymous. Public-key encryption flawed in time. *Network Security*, 1996(1): 3, January 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901531.

Anonymous:1996:SAB

[Ano96x] Anonymous. SecurID authentication for BayRS routers. *Network Security*, 1996(3):4, March 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901233.

Anonymous:1996:SAO

[Ano96y] Anonymous. Security and authentication offered. *Network Security*, 1996(7):3–4, July 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896900938.

Anonymous:1996:SCG

[Ano96z] Anonymous. Smart cards get wise. *IEEE Micro*, 16(1):4, January/February 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Anonymous:1996:SAS

[Ano96-27] Anonymous. SoftID authentication software. *Network Security*, 1996(6): 6, June 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901476.

Anonymous:1996:SUS

[Ano96-28] Anonymous. Standards update: Standardization efforts for triple-DES continue; IEEE P1363 works toward integrated draft; PKCS #11 / Cryptoki Workshop held at MIT; more progress on S/MIME. *CryptoBytes*, 2(2):11–12, Summer 1996. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n2.pdf.

Anonymous:1996:TBAa

[Ano96-29] Anonymous. Technology and business: Artificial blood starts circulating. fishermen sound off for porpoises. encryption chaos continues. *Scientific American*, 275(3):40–??, September 1996. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/0996issue/0996currentissue.html.

Anonymous:1996:TBSa

[Ano96-30] Anonymous. Technology and business: The scoop on plutonium processing military prototypes in Bosnia. public-key encryption at risk. *Scientific American*, 274(3):12–??, March 1996. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/0396issue/0396toc.html.

Anonymous:1996:UDE

[Ano96-31] Anonymous. Users demand encryption policies. *Network Security*, 1996(1):5, January 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901609.

Anonymous:1997:RDSa

[Ano97a] Anonymous, editor. *1997 RSA Data Security Conference, 28–31 January 1997, San Francisco, California*. RSA Data Security, Inc., Redwood City, CA, USA, 1997. LCCN ????

Anonymous:1997:AES

[Ano97b] Anonymous. Advanced Encryption Standard, draft minimum requirements and evaluation criteria. *Lecture Notes in Computer Science*, 1267:83–87, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670083.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670083.pdf.

Anonymous:1997:AUC

[Ano97c] Anonymous. Algorithms update: DES challenge solved; RC2 published in IETF Forum. *CryptoBytes*, 3(1):14, Spring 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n1.pdf.

Anonymous:1997:AWS

[Ano97d] Anonymous. All the Web's a stage — trusted Web, a one-step authentication server. *BYTE Magazine*, 22(8):135–??, August 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1997:AIR

[Ano97e] Anonymous. Announcements: In this issue: The

RSA Data Security Factoring Challenge; the RSA Data Security Secret-Key Challenge. *CryptoBytes*, 2 (3):16, Winter 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n3.pdf.

Anonymous:1997:ARDa

[Ano97f] Anonymous. Announcements: The RSA Data Security Conference '98. *CryptoBytes*, 3(1):16, Spring 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n1.pdf.

Anonymous:1997:ARDb

[Ano97g] Anonymous. Announcements: The RSA Data Security Conference '98. *CryptoBytes*, 3(2):16, Autumn 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n2.pdf.

Anonymous:1997:ADF

[Ano97h] Anonymous. Announcing development of a Federal Information Processing Standard for Advanced Encryption Standard. *Federal Register*, 62(1):93–94, January 2, 1997. CODEN FEREAC. ISSN 0097-6326.

Anonymous:1997:BUF

[Ano97i] Anonymous. Breakthrough for UK firm with US encryption restrictions. *Network Security*, 1997(6): 5, June 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897895219.

Anonymous:1997:CFG

[Ano97j] Anonymous. Companies form group to support cross-platform encryption. *Network Security*, 1997(2): 4, February 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/1353485897900593.

Anonymous:1997:CKG

[Ano97k] Anonymous. Cryptography: a key to growth — and crime: Nicholas Bray, Wall Street Journal Europe, January 27, 1997. *Computers and Security*, 16(1): 62, ???? 1997. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404897857914.

Anonymous:1997:CVC

[Ano97l] Anonymous. Cyber view: Is a code cracker a concealed weapon? *Scientific American*, 276(4): 42–??, April 1997. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/

0497issue/0497currentissue.html.

Anonymous:1997:DEU

[Ano97m] Anonymous. Desktop encryption utility. *Network Security*, 1997(1):7, January 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897835040.

Anonymous:1997:DHE

[Ano97n] Anonymous. Diffie–Hellman encryption freely available. *Network Security*, 1997(12):5, December 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897900842.

Anonymous:1997:DNH

[Ano97o] Anonymous. The distributed.net home page. Contains announcement of a prize for cracking DES. The prize was claimed five months later [Ele98, p. xi]., June 17, 1997. URL http://www.distributed.net/des/; http://www.frii.com/~rcv/deschall.htm.

Anonymous:1997:EAS

[Ano97p] Anonymous. Easy authentication and signature verification. *Network Security*, 1997(4):6, April 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897800013.

Anonymous:1997:ENa

[Ano97q] Anonymous. Editor's note. *CryptoBytes*, 2(3):2, Winter 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n3.pdf.

Anonymous:1997:ENb

[Ano97r] Anonymous. Editor's note. *CryptoBytes*, 3(1):2, Spring 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n1.pdf.

Anonymous:1997:ENc

[Ano97s] Anonymous. Editor's note. *CryptoBytes*, 3(2):2, Autumn 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n2.pdf.

Anonymous:1997:EAJ

[Ano97t] Anonymous. Encryption and authentication for Java. *Network Security*, 1997(6):6, June 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897895256.

Anonymous:1997:ECR

[Ano97u] Anonymous. Encryption compromise on rocky ground. *Network Security*, 1997(1):4–5, January 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897834940.

Anonymous:1997:EKB

[Ano97v] Anonymous. Encryption key of 48 bits cracked. *Network Security*, 1997(3): 2, March 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897830310.

Anonymous:1997:EW

[Ano97w] Anonymous. Enforcing watermarks. *BYTE Magazine*, ??(??):??, January 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic). URL http://www.byte.com/art/9701/sec18/art4.htm.

Anonymous:1997:FSU

[Ano97x] Anonymous. File security uses smartcard and RSA encryption. *Network Security*, 1997(4):5, April 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897899990.

Anonymous:1997:FCR

[Ano97y] Anonymous. French companies restricted from using high-end encryption. *Network Security*, 1997(3): 3, March 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348589783036X.

Anonymous:1997:HEW

[Ano97z] Anonymous. How to embed a watermark. *BYTE Magazine*, ??(1):??, January 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic). URL http://www.byte.com/art/9701/sec18/art3.htm.

Anonymous:1997:HDR

[Ano97-27] Anonymous. HTML-driven remote authentication. *Network Security*, 1997(9):6, September 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897900209.

Anonymous:1997:INI

[Ano97-28] Anonymous, editor. *Issues for networked interpersonal communicators: Colloquium — May 1997, London*, number 139 in COL-

LOQUIUM DIGEST- IEE 1997. IEE, London, UK, 1997. ISSN 0963-3308. LCCN ????

Anonymous:1997:MNL

[Ano97-29] Anonymous. Micro news: Lattice cryptography, domain name antitrust investigation. *IEEE Micro*, 17(4):2–??, July/August 1997. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL `http://pascal.computer.org/mi/books/mi1997/pdf/m4002.pdf`.

Anonymous:1997:MLE

[Ano97-30] Anonymous. Military-level encryption for all data transmissions. *Network Security*, 1997(10):6, October 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485897901045`.

Anonymous:1997:MEP

[Ano97-31] Anonymous. Ministry's encryption policy criticized. *Network Security*, 1997(10): 3–4, October 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485897900970`.

Anonymous:1997:NPP

[Ano97-32] Anonymous. New 'plug and play' cryptographic accelerators available. *Network Security*, 1997(11):6, November 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S135348589790074X`.

Anonymous:1997:NPA

[Ano97-33] Anonymous. New products: AcceleratedX Server Version 3.1; CDE Business Desktop; DNEWS News Server 4.0; SecureNet PRO v2.0; Dynamic Modules; Stronghold Encrypting SSL Web Server; SOLID Desktop; Lone Star LONE-TAR 2.2gn Shop; Cactus System Crash AIR-BAG 3.4.1.1. *Linux Journal*, 39:??, July 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Anonymous:1997:NPNb

[Ano97-34] Anonymous. New products: NetTracker 3.0; ScriptEase: Integration SDK; JDesignerPro 2.1; VirtuFlex 2.0; PGP Version 5.0 for Personal Privacy; TeraSpell 97; FileDrive File Transfer Server; journyx WebTime. *Linux Journal*, 43:??, November 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Anonymous:1997:PEH

[Ano97-35] Anonymous. PGP encryption heavily criticized. *Network Security*, 1997(3): 3, March 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897830358.

Anonymous:1997:RAS

[Ano97-36] Anonymous. Remote access solution to encrypt data. *Network Security*, 1997(5): 8, May 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897900465.

Anonymous:1997:RCU

[Ano97-37] Anonymous. Reviews and commentaries: An updated history of cryptology "forgotten genius" Nikola Tesla; archaeological eyewitnesses. *Scientific American*, 276(4): 108–??, April 1997. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/0497issue/0497currentissue.html.

Anonymous:1997:RAJ

[Ano97-38] Anonymous. RSA announces Java encryption tool kit. *SunServer*, 11(11): 19, November 1997. ISSN 1091-4986.

Anonymous:1997:RDL

[Ano97-39] Anonymous. RSA Data licenses Java encryption library. *Cisco World: The Independent Journal for Internetworking Professionals*, 3(8):21, August 1997. ISSN 1081-3187.

Anonymous:1997:RDSb

[Ano97-40] Anonymous. The RSA Data Security DES Challenge II. *CryptoBytes*, 3 (2):8, Autumn 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n2.pdf.

Anonymous:1997:RBE

[Ano97-41] Anonymous. RSA's 40-bit encryption algorithm cracked. *Network Security*, 1997(2):3, February 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348589786638X.

Anonymous:1997:SFR

[Ano97-42] Anonymous. Security: The Federal Reserve is testing an Advanced Data Encryption Standard. *Bank systems + technology*, 34(6): 18–??, 1997. CODEN BSYTEE. ISSN 1045-9472.

Anonymous:1997:SAP

[Ano97-43] Anonymous. SecurlD authentication protects corporate information. *Net-*

work Security, 1997(8):6–7, August 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897832369.

Anonymous:1997:SUE

[Ano97-44] Anonymous. Standards update: Extensive revisions to PKCS underway; P1363 work continues. *CryptoBytes*, 3(1):15, Spring 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n1.pdf.

Anonymous:1997:SUR

[Ano97-45] Anonymous. Standards update: RC5 is published as an Internet RFC; successor to DES sought; progress on P1363 continues. *CryptoBytes*, 2(3):13, Winter 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n3.pdf.

Anonymous:1997:SEA

[Ano97-46] Anonymous. Strong encryption available worldwide. *Network Security*, 1997(4):3–4, April 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897899965.

Anonymous:1997:SSA

[Ano97-47] Anonymous. Su, Siemens agree to embed Java into smartcard chips. *SunServer*, 11(9):19, September 1997. ISSN 1091-4986.

Anonymous:1997:CBP

[Ano97-48] Anonymous. The Colossus of Bletchley Park, IEEE Rev., vol. 41, no. 2, pp. 55–59 [book reviews]. *IEEE Annals of the History of Computing*, 19(1):80, January–March 1997. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL http://ieeexplore.ieee.org/iel4/85/12228/00560758.pdf.

Anonymous:1997:TER

[Ano97-49] Anonymous. Tightening of encryption regulations in Japan. *Network Security*, 1997(1):4, January 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897834927.

Anonymous:1997:UUS

[Ano97-50] Anonymous. *Undang-undang siber: Akta Tandatangan Digital 1997, Akta Jenayah Komputer 1997, Akta Teleperubatan 1997 = Cyber laws: Digital Signature Act 1997, Computer Crimes Act 1997,* *Telemedicine Act 1997*. Undang-undang Malaysia. Percetakan Nasional Malaysia, Kuala Lumpur, 1997. various pp.

Anonymous:1997:UEL

[Ano97-51] Anonymous. US export licence for 128-bit encryption for Microsoft. *Network Security*, 1997(7): 7, July 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S135348589789873X`.

Anonymous:1997:UPP

[Ano97-52] Anonymous. USACM participates in protest against restrictions on cryptography research and development. *Communications of the Association for Computing Machinery*, 40(11(S)):5–??, November 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Anonymous:1997:VPA

[Ano97-53] Anonymous. Vulnerabilities in pluggable authentication module. *Network Security*, 1997(5):3, May 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485897856899`.

Anonymous:1998:ABF

[Ano98a] Anonymous. Alliance brings full strength encryption to Europe. *Network Security*, 1998(4): 5, April 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485898901015`.

Anonymous:1998:ARD

[Ano98b] Anonymous. Announcements: The RSA Data Security Conference '99. *CryptoBytes*, 4(1):24, Summer 1998. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto4n1.pdf`.

Anonymous:1998:CSIb

[Ano98c] Anonymous. Computer security and the Internet. *Scientific American*, 279 (4):95–95 (Intl. ed. 69–??), October 1998. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.sciam.com/1998/1098issue/1098currentissue.html`.

Anonymous:1998:CPP

[Ano98d] Anonymous. Crypto pack protects electronic information. *Network Security*, 1998(7):6, July 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http:/`

/www.sciencedirect.com/science/article/pii/S135348589890040X.

Anonymous:1998:CASb

[Ano98e] Anonymous. Cryptographic accelerator for speedy digital signatures. *Network Security*, 1998(9):4, September 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898901301.

Anonymous:1998:CASa

[Ano98f] Anonymous. Cryptographic accelerators support key management. *Network Security*, 1998(2):4, February 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898900861.

Anonymous:1998:CDR

[Ano98g] Anonymous. The cryptographic debate rages on. *Network Security*, 1998(4):5, April 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898901003.

Anonymous:1998:CSCb

[Ano98h] Anonymous. Cryptographic solution for e-commerce security. *Network Security*, 1998(5):5, May 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898901751.

Anonymous:1998:ICS

[Ano98i] Anonymous. DES-II challenges solved. *CryptoBytes*, 4(1):23, Summer 1998. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n1.pdf.

Anonymous:1998:EN

[Ano98j] Anonymous. Editor's note. *CryptoBytes*, 4(1):2, Summer 1998. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n1.pdf.

Anonymous:1998:EWB

[Ano98k] Anonymous. Encryption for Web-based banking applications. *Network Security*, 1998(3):4, March 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898901180.

Anonymous:1998:Ea

[Ano98l] Anonymous. Eurocrypt '83. *Lecture Notes in Computer Science*, 1440:21–22, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/

link/service/series/0558/bibs/1440/14400021.htm; http://link.springer-ny.com/link/service/series/0558/papers/1440/14400021.pdf.

Anonymous:1998:LEE

[Ano98m] Anonymous. Link encryptor with electronically loadable algorithms. *Network Security*, 1998(11):6, November 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348589890054X.

Anonymous:1998:PCA

[Ano98n] Anonymous, editor. *Proceedings of the 105th Convention of the Audio Engineering Society, San Francisco, USA 26–29 September, 1998*. Audio Engineering Society, New York, NY, USA, 1998. LCCN ????

Anonymous:1998:SEF

[Ano98o] Anonymous. Safety of encrypted files questioned. *Network Security*, 1998(1):4–5, January 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898901581.

Anonymous:1998:SIb

[Ano98p] Anonymous. The Smartcard invasion. *BYTE Magazine*, 23(1):76–??, January 1998. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1998:SIC

[Ano98q] Anonymous. Smartcard invasion continues — security applications will be the spearhead for these "credit cards with brains.". *BYTE Magazine*, 23(4):112C–??, April 1998. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1998:SUP

[Ano98r] Anonymous. Standards update: PKCS standards; IEEE P1363. *CryptoBytes*, 4(1):11, Summer 1998. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n1.pdf.

Anonymous:1998:SAP

[Ano98s] Anonymous. Strong authentication protects Windows NT. *Network Security*, 1998(5):4–5, May 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348589890174X.

Anonymous:1998:TBF

[Ano98t] Anonymous. Technology and business: a fast Y2K bug fix. confidentiality without encryption…

Earthcam.com. *Scientific American*, 278(6):34–??, June 1998. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/1998/0698issue/0698currentissue.html.

Anonymous:1998:UGT

[Ano98u] Anonymous. UK Government to toughen encryption regulations. *Network Security*, 1998(11):3–4, November 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898900484.

Anonymous:1998:UFR

[Ano98v] Anonymous. US finally relaxes encryption policies. *Network Security*, 1998(10):2–3, October 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898901817.

Anonymous:1999:RDS

[Ano99a] Anonymous. The 1999 RSA data security conference. *CryptoBytes*, 4(2):20, Winter 1999. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n2.pdf.

Anonymous:1999:AWS

[Ano99b] Anonymous. Announcement: *Workshop on Smartcard Technology. ;login: the USENIX Association newsletter*, 24(2):??, April 1999. CODEN LOGNEM. ISSN 1044-6397.

Anonymous:1999:CCI

[Ano99c] Anonymous, editor. *Cool Chips II: An International Symposium on Low-Power and High-Speed Chips: Kyoto Research Park. Kyoto, Japan on April 26–27, 1999.* ????, ????, 1999.

Anonymous:1999:CEV

[Ano99d] Anonymous. Cylink expands its VPN offerings with ATM encryptor. *Network Security*, 1999(8):4–5, August 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348589990034X.

Anonymous:1999:DSC

[Ano99e] Anonymous. Delegation and not-so smart cards: Discussion. *Lecture Notes in Computer Science*, 1550:158–167, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anonymous:1999:DSV

[Ano99f] Anonymous. DREO secure video conferencing and high speed data encryption tests for Inmarsat-B satellite terminals. Technical memorandum AD-a371 256, Defence Research Establishment Ottawa, Ottawa, ON, Canada, 1999. 51 pp.

Anonymous:1999:EDB

[Ano99g] Anonymous. Encrypt data at 6.7 billion bits per second. *Network Security*, 1999 (8):5, August 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899900351.

Anonymous:1999:EPFa

[Ano99h] Anonymous. Encryptors provide frame relay security. *Network Security*, 1999 (5):5, May 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899902854.

Anonymous:1999:EGC

[Ano99i] Anonymous. Entrust gets contract to provide authenticity. *Network Security*, 1999(1):5, January 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899901940.

Anonymous:1999:KNT

[Ano99j] Anonymous. Key note: Trust management for public-key infrastructures: Discussion-trust management. *Lecture Notes in Computer Science*, 1550: 64–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anonymous:1999:L

[Ano99k] Anonymous. L'inuktitut. World-Wide Web document., 1999. URL http://colourlab.com/arctic/inuktitut.htm; http://www.culture.fr/edm/fr/index.html. Follow the navigation panel link "Les écritures" to inuktitut. The author observes that the syllabary used for the Inuit language, Inuktitut, was created at the end of the 19th Century by James Evans, a Wesleyan missionary, inspired by *stenography*. Originally intended for transcription of the Objiway language, it was later used for Cree and Inuktitut; only these three languages have been written in this syllabary. Examples of the syllabary are shown in links that can be followed from this page; another alphabet table is shown in the colourlab.com URL.

Anonymous:1999:SFU

[Ano99l] Anonymous. Secure fingerprinting using public-key cryptography: Discussion. *Lecture Notes in Computer Science*, 1550:90–94, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anonymous:1999:ULE

[Ano99m] Anonymous. US lifts export curbs on encryption. *Network Security*, 1999(10): 3, October 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899901721.

Anonymous:1999:WDE

[Ano99n] Anonymous. Wireless data encryption for handhelds. *Network Security*, 1999(9): 3, September 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899902532.

ANSI:1997:AXP

[ANS97] ANSI. *ANSI X9.30-2:1997: Public Key Cryptography Using Irreversible Algorithms — Part 2: The Secure Hash Algorithm (SHA-1)*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, 1997. URL http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9%2E30%2D2%3A1997.

Anderson:1998:SFS

[ANS98a] Ross J. Anderson, Roger M. Needham, and Adi Shamir. The steganographic file system. *Lecture Notes in Computer Science*, 1525: 73–82, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250073.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250073.pdf.

ANSI:1998:AXD

[ANS98b] ANSI. *ANSI X9.31:1998: Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, 1998. URL http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9%2E31%3A1998.

Anderson:1996:CCA

[AO96] M. S. Anderson and M. A. Ozols. Covert channel analysis for stubs. In Anderson [And96c], pages 95–113. CODEN

LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054202.html.

Abbott:1993:INT

[AP93] Mark B. Abbott and Larry L. Peterson. Increasing network throughput by integrating protocol layers. *IEEE/ACM Transactions on Networking*, 1(5):600–610, October 1993. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL http://www.acm.org:80/pubs/citations/journals/ton/1993-1-5/p600-abbott/.

Abreu:1994:DAI

[AP94] S. Abreu and L. M. Pereira. Design for AKL with intelligent pruning. *Lecture Notes in Computer Science*, 798:3–10, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anderson:1998:LS

[AP98] R. J. Anderson and F. A. P. Petitcolas. On the limits of steganography. *IEEE Journal on Selected Areas in Communications*, 16(4):463–473, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072102.html.

Andrasiu:1993:LTP

[APDS93] Mircea Andraşiu, Gheorghe Păun, Jürgen Dassow, and Arto Salomaa. Language-theoretic problems arising from Richelieu cryptosystems. *Theoretical Computer Science*, 116(2):339–357, August 16, 1993. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1993&volume=116&issue=2&aid=1238.

Aruliah:1985:PIE

[APW85] A. A. Aruliah, G. I. Parkin, and Brian A. Wichmann. A Pascal implementation of the DES encryption algorithm including cipher block chaining. NPL report DITC 61/85, National Physical Laboratory, Division of Information Technology and Computing, Teddington, Middlesex, UK, 1985. 37 pp.

Allen:1997:PSA

[AR97] Robert B. Allen and Edie M. Rasmussen, editors. *Proceedings of the second ACM International Conference on Digital Libraries:*

ACM Digital Libraries '97, Philadelphia, PA, July 23–26, 1997. ACM Press, New York, NY 10036, USA, 1997. ISBN 0-89791-868-1. LCCN Z 699 A1 A27 1997. ACM order number 606971.

Aumann:1998:AES

[AR98] Yonatan Aumann and Michael O. Rabin. Authentication, enhanced security and error correcting codes. *Lecture Notes in Computer Science*, 1462: 299–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620299.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620299.pdf`.

Aumann:1999:ITS

[AR99] Y. Aumann and M. O. Rabin. Information theoretically secure communication in the limited storage space model. In Wiener [Wie99], pages 65–79. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Arazi:1993:AEA

[Ara93] B. Arazi. Architectures for exponentiation over GD(2^n) adopted for smartcard application. *IEEE Transactions on Computers*, 42 (4):494–497, April 1993. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=214694`.

Arensberg:1921:CD

[Are21] Walter Arensberg. *The cryptography of Dante*. Alfred A. Knopf, New York, NY, USA, 1921. x + 494 pp. LCCN PQ4406.A7.

Arensberg:1922:CSP

[Are22] Walter Arensberg. *The cryptography of Shakespeare. Part one*. Howard Bowen, Los Angeles, CA, USA, 1922. ix + 280 pp. LCCN PR2944.A6. No more published. Source: Bequest of George Fabyan, 1940. DLC.

Adamson:1995:JSR

[ARH95] William A. Adamson, Jim Rees, and Peter Honeyman. Joining security realms: a single login for NetWare and Kerberos. In USENIX Association [USE95b], pages 157–166. ISBN 1-880446-70-7. LCCN QA76.8.U65 U55 1992(3)-1995(5). URL `http://www.usenix.org/publications/library/proceedings/security95/adamson.html`.

Abdulla:1999:OMS

[ARK99] M. F. Abdulla, C. P. Ravikumar, and Anshul Kumar. Optimization of mutual and signature testing schemes for highly concurrent systems. *Communications of the Association for Computing Machinery*, 42(3):199–216, March 1999. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org:80/pubs/citations/journals/cacm/1999-42-3/p199-abdulla/.

Adleman:1999:AMC

[ARRW99] Leonard M. Adleman, Paul W. K. Rothemund, Sam Roweis, and Erik Winfree. On applying molecular computation to the Data Encryption Standard. In *DNA based computers, II (Princeton, NJ, 1996)*, volume 44 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 31–44. Amer. Math. Soc., Providence, RI, 1999.

Adleman:1983:CCS

[ARS83] L. M. Adleman, R. L. Rivest, and A. Shamir. Cryptographic communications system and method. US Patent No. 4,405,829., September 20, 1983. URL https://www.google.com/patents/US4405829. Patent filed 14 September 1977.

Aiello:1999:HPN

[ARV99a] W. Aiello, S. Rajagopalan, and R. Venkatesan. High-speed pseudorandom number generation with small memory. In Knudsen [Knu99c], pages 290–304. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Aiello:1999:HSP

[ARV99b] W. Aiello, S. Rajagopalan, and R. Venkatesan. High-speed pseudorandom number generation with small memory. *Lecture Notes in Computer Science*, 1636: 290–304, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alpern:1983:KEU

[AS83] B. Alpern and F. B. Schneider. Key exchange using keyless cryptography. *Information Processing Letters*, 16(2):79–81, February 26, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Atici:1996:UHM

[AS96] M. Atici and Douglas R. Stinson. Universal hashing and multiple authentication. *Lecture Notes in Computer Science*, 1109:

16–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090016.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090016.pdf.

Ashenhurst:1987:ATA

[Ash87] Robert L. Ashenhurst, editor. *ACM Turing Award Lectures: the first twenty years, 1966–1985*. ACM Press anthology series. ACM Press and Addison-Wesley, New York, NY 10036, USA and Reading, MA, USA, 1987. ISBN 0-201-07794-9. xviii + 483 pp. LCCN QA76.24 .A33 1987.

Araki:1998:OEC

[ASM98] K. Araki, T. Satoh, and S. Miura. Overview of elliptic curve cryptography. *Lecture Notes in Computer Science*, 1431:29–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

USENIX:1988:CSSb

[Ass88] USENIX Association, editor. *Computing Systems, Summer, 1988*. USENIX Association, Berkeley, CA, USA, Summer 1988.

Asokan:1998:OFE

[ASW98] N. Asokan, Victor Shoup, and Michael Waidner. Optimistic fair exchange of digital signatures (extended abstract). *Lecture Notes in Computer Science*, 1403: 591–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030591.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030591.pdf.

Abdalla:1999:TMB

[ASW99] Michel Abdalla, Yuval Shavitt, and Avishai Wool. Towards making broadcast encryption practical. In Franklin [Fra99], pages 140–157. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999. URL http://link.springer-ny.com/link/service/series/0558/bibs/1648/16480140.htm; http://link.springer-ny.com/link/service/series/0558/papers/1648/16480140.pdf.

Atkins:1996:RPM

[ASZ96] D. Atkins, W. Stallings, and P. Zimmermann. RFC 1991: PGP message exchange formats, August 1996. URL ftp://ftp.internic.net/rfc/rfc1991.txt; https:

//www.math.utah.edu/pub/rfc/rfc1991.txt. Status: INFORMATIONAL.

Akl:1983:CSP

[AT83] Selim G. Akl and Peter D. Taylor. Cryptographic solution to a problem of access control in a hierarchy. *ACM Transactions on Computer Systems*, 1(3):239–248, August 1983. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Ateniese:1999:SOI

[AT99] G. Ateniese and G. Tsudik. Some open issues and new directions in group signatures. In Franklin [Fra99], pages 196–211. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Atallah:1999:ATC

[Ata99] Mikhail J. Atallah, editor. *Algorithms and theory of computation handbook*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1999. ISBN 0-8493-2649-4. various pp. LCCN QA76.9.A43A43 1999.

Atanasiu:1993:AEU

[Ata94] Adrian Atanasiu. About encryption using formal methods—substitution on words and languages. *An. Univ. Bucureşti Mat. Inform.*, 42/43:68–75, 1993/94. ISSN 1224-7170.

Al-Tawil:1998:NAP

[ATAY98] K. Al-Tawil, A. Akrami, and H. Youssef. A new authentication protocol for GSM networks. In IEEE Computer Society. Technical Committee on Computer Communications [IEE98f], pages 21–30. ISBN 0-8186-8810-6, 0-8186-8818-1 (microfiche). LCCN TK5105.5 .C66 1998. IEEE Computer Society Press Order Number PR08810. IEEE Order Plan Catalog Number 98TB100260.

Atkins:1993:CKE

[Atk93] Derek A. (Derek Allan) Atkins. Charon: Kerberos extensions for authentication over secondary networks. Thesis (B.S.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1993. vii + 91 pp.

Atkinson:1995:RIA

[Atk95a] R. Atkinson. RFC 1826: IP authentication header, August 1995. URL ftp://ftp.internic.net/rfc/rfc1826.txt; https://www.math.utah.edu/pub/rfc/rfc1826.txt. Obsoleted by RFC2402 [KA98a]. Status: PROPOSED STANDARD.

Atkinson:1995:RIE

[Atk95b] R. Atkinson. RFC 1827: IP encapsulating security payload (ESP), August 1995. URL ftp://ftp.internic.net/rfc/rfc1827.txt; https://www.math.utah.edu/pub/rfc/rfc1827.txt. Obsoleted by RFC2406 [KA98b]. Status: PROPOSED STANDARD.

Atkinson:1997:TMS

[Atk97] Randall J. Atkinson. Toward a more secure Internet. *Computer*, 30(1):57–61, January 1997. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

ATT:1986:AUS

[AT&T86] AT&T. *AT&T UNIX System Readings and Applications*, volume II. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1986. ISBN 0-13-939845-7. xii + 324 pp. LCCN QA76.76.O63 U553 1986.

Aucsmith:1996:TRS

[Auc96] D. Aucsmith. Tamper-resistant software: An implementation. In Anderson [And96c], pages 317–333. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054104.html.

Aucsmith:1998:SIW

[Auc98] David Aucsmith, editor. *Second International Workshop on Information Hiding, 14–17 April, 1998, Portland, Oregon, USA*, volume 1525 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-65386-4. LCCN QA76.9.A25I48 1998.

Aura:1996:PID

[Aur96] T. Aura. Practical invisibility in digital communications. In Anderson [And96c], pages 265–278. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054105.html.

AAGD:1996:RPR

[Aus96] Australia.Attorney-General's Dept. *Review of policy relating to encryption technologies*. Australian Govt. Pub. Service, Canberra, ACT, Australia, October 10, 1996. ISBN 0-644-47530-7. xii + 96 pp. LCCN ???? A.G.P.S. cat. no. 96 0799 4.

Aparicio:1999:ITD

[AVLPF99] P. Aparicio, R. Ventura, P. Lima, and C. Pinto-Ferreira. ISocRob — team description. *Lecture Notes in Computer Science*, 1604: 434–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Avolio:1998:PCP

[Avo98] Frederick M. Avolio. Practical cryptography — privacy for business and electronic commerce, 1998. URL http://www.usenix.org/publications/library/proceedings/lisa98/invited_talks/avolio_html/. Unpublished invited talk at the 12th Systems Administration Conference (LISA '98) December 6–11, 1998 Boston, Massachusetts, USA.

Anderson:1996:NC

[AVPN96] R. Anderson, S. Vaudenay, B. Preneel, and K. Nyberg. The Newton channel. In Anderson [And96c], pages 151–156. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054603.html.

Alabbadi:1994:SDS

[AW94] M. Alabbadi and S. B. Wicker. Susceptibility of digital signature schemes based on error-correcting codes to universal forgery. *Lecture Notes in Computer Science*, 829:6–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alabbadi:1995:DSS

[AW95] M. Alabbadi and S. B. Wicker. A digital signature scheme based on linear error-correcting block codes. *Lecture Notes in Computer Science*, 917: 238–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Angel:1999:JQH

[AW99] Dave Angel and Andy Wilson. Java Q and A: How do I store a Java app in a self-executing encrypted file? *Dr. Dobb's Journal of Software Tools*, 24 (2):115–116, 118, 120–121, February 1999. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/1999/9902/9902toc.htm; http://www.ddj.com/ftp/1999/1999_02/jqa299.txt; http://www.ddj.com/ftp/1999/1999_02/jqa299.zip.

Aspray:1988:RCD

[AWL+88] William Aspray, Maurice V. Wilkes, Albert C. Lewis, Greg Mellen, Harold Chucker, Robert V. D. Campbell, Wendy Wilkins, G. J. Tee, Ernest Braun, and Arthur L. Norberg. Reviews: Carpenter and Doran (eds.): A. M. Turing's ACE Report of 1946 and Other Papers; Masani (ed.): Norbert Wiener: Collected Works with Commentaries; Kozaczuk: Enigma: How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two; Worthy: William C. Norris: Portrait of a Maverick; Harvard Computation Laboratory: A Manual of Operation for the Automatic Sequence Controlled Calculator; Proceedings of a Symposium on Large-Scale Digital Calculating Machinery; Gardner: The Mind's New Science: A History of the Cognitive Revolution; Hartree: Calculating Machines: Recent and Prospective Developments and Their Impact on Mathematical Physics and Calculating Instruments and Machines; McLean and Rowland: The Inmos Saga; Pennings and Buifendam (eds.): New Technology as Organizational Innovation: The Development and Diffusion of Microelectronics; other literature. *Annals of the History of Computing*, 10(1):80–97, January/March 1988. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1988/pdf/a1080.pdf`; `http://www.computer.org/annals/an1988/a1080abs.htm`. See minor erratum [Ano88h]: Hartree as a mathematical physicist, not a physical chemist.

AufderHeide:1999:PGP

[AWV99] F. M. Auf der Heide, M. Westermann, and B. Voecking. Provably good and practical strategies for non-uniform data management in networks. *Lecture Notes in Computer Science*, 1643: 89–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ayoub:1968:EKR

[Ayo68a] F. Ayoub. Encryption with keyed random permutations. *Electronics Letters*, 17(??):583–585, February 1968. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4245887`.

Ayoub:1968:EEK

[Ayo68b] F. Ayoub. Erratum: Encryption with keyed random permutations. *Electronics Letters*, 17(??): ??, February 1968. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4246020.

Ayoub:1981:EKR

[Ayo81] F. Ayoub. Encryption with keyed random permutations. *Electronics Letters*, 17(17):583–585, 1981. CODEN ELLEAK. ISSN 0013-5194.

Ayoub:1983:DCE

[Ayo83] F. Ayoub. The design of complete encryption networks using cryptographically equivalent permutations. *Computers and Security*, 2(3):261–267, November 1983. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488390010X.

Bernstein:1996:ISB

[B+96a] Terry Bernstein et al. *Internet security for business*. John Wiley and Sons, Inc., New York, NY, USA, 1996. ISBN 0-471-13752-9 (paperback). various pp. LCCN HD30.38.I57 1996.

Blau:1996:VPA

[B+96b] Brian Blau et al., editors. *Visual proceedings: the art and interdisciplinary programs of SIGGRAPH 96: SIGGRAPH 96, August 4–9, 1996, New Orleans, LA*, Computer Graphics. ACM Press, New York, NY 10036, USA, 1996. ISBN 0-89791-784-7. ISSN 1069-5419. LCCN T385 .S54 1996b. URL http://info.acm.org/pubs/contents/proceedings/graph/.

Baker:1997:RRM

[BA97] F. Baker and R. Atkinson. RFC 2082: RIP-2 MD5 authentication, January 1997. URL ftp://ftp.internic.net/rfc/rfc2082.txt; https://www.math.utah.edu/pub/rfc/rfc2082.txt. Status: PROPOSED STANDARD.

Bach:1988:HGF

[Bac88] Eric Bach. How to generate factored random numbers. *SIAM Journal on Computing*, 17(2):179–193, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Bacard:1995:CPH

[Bac95] André Bacard. *Computer Privacy Handbook: a Practical Guide to E-Mail Encryption*. Peachpit Press, Inc., 1085 Keith Avenue, Berkeley, CA 94708, USA, 1995. ISBN 1-56609-171-3. 274 pp. LCCN ???? US$24.95.

Badia:1999:EDL

[Bad99] A. Badia. Extending description logics with generalized quantification. *Lecture Notes in Computer Science*, 1609:94–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Baker:1992:CAB

[Bak92] H. G. Baker. Computing $A * B \pmod{N}$ efficiently in ANSI C. *ACM SIGPLAN Notices*, 27(1):95–98, January 1992. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Biham:1998:SNB

[BAK98] E. Biham, R. Anderson, and L. R. Knudsen. Serpent: a new block cipher proposal. *Lecture Notes in Computer Science*, 1372:222–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bakker:1999:MAS

[Bak99] Bastiaan Bakker. Mutual authentication with Smart Cards. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL `http://www.usenix.org/publications/library/proceedings/smartcard99/bakker.html`.

Ball:1997:ESS

[Bal97] Steve Ball. An encryption system for software registration. *C/C++ Users Journal*, 15(2):55–??, February 1997. CODEN CCUJEX. ISSN 1075-2838.

Ball:1999:WSB

[Bal99] Jimmy Ball. Web security basics with Apache: Authentication and secure log files. *Sys Admin: The Journal for UNIX Systems Administrators*, 8(2): 43–46, February 1999. CODEN SYADE7. ISSN 1061-2688. URL `http://www.samag.com/`.

Bullitt:1999:GDI

[BALS99] E. Bullitt, S. Aylward, A. Liu, and J. Stone. 3D graph description of the intracerebral vasculature from segmented MRA and tests of accuracy by comparison with X-ray angiograms. *Lecture Notes in Computer Science*, 1613: 308–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bamford:1982:PPR

[Bam82] James Bamford. *The puzzle palace: a report on America's most secret agency.*

Houghton-Mifflin, Boston, MA, USA, 1982. ISBN 0-395-31286-8. 465 pp. LCCN KF7683.N32 B3.

Bamforth:1997:JSS

[Bam97] R. Bamforth. Java — from smartcard to supercomputer. In Anonymous [Ano97-28], pages 1–?? ISSN 0963-3308. LCCN ????

Burrows:1989:LAb

[BAN89a] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *Operating Systems Review*, 23(5):1–13, December 1989. CODEN OSRED8. ISSN 0163-5980.

Burrows:1989:LAa

[BAN89b] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. Technical Report 39, Digital Equipment Corporation, Systems Research Centre, February 28, 1989. 48 pp.

Burrows:1990:LA

[BAN90] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1): 18–36, February 1990. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tocs/1990-8-1/p18-burrows/`.

Banisar:1993:BCE

[Ban93] David Banisar. Battle for control of encryption technology. *IEEE Software*, 10 (4):95–97, July 1993. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Banisar:1994:CPS

[Ban94] David Banisar. *1994 cryptography and privacy sourcebook: primary documents on U.S. encryption policy, the Clipper Chip, the Digital Telephony Proposal and export controls*. Diane Publishing, Upland, PA, USA, 1994. ISBN 0-7881-0829-8 (paperback). various pp. LCCN ????

Bao:1994:IRL

[Bao94] Feng Bao. Increasing ranks of linear finite automata and complexity of FA public key cryptosystem. *Sci. China Ser. A*, 37(4):504–512, 1994. ISSN 1001-6511.

Barker:1961:CSC

[Bar61] Wayne G. Barker. *Cryptanalysis of the single columnar transposition cipher*. C. E. Tuttle Co., Rutland, VT, USA, 1961. x + 1 + 140 pp. LCCN Z103 Z32.

Bartek:1974:EDS

[Bar74] Douglas J. Bartek. Encryption for data security. *Hon-*

eywell Computer Journal, 8 (2):86–89, ???? 1974. CODEN HNCJA3. ISSN 0046-7847.

Barker:1975:CSS

[Bar75] Wayne G. Barker. *Cryptanalysis of the simple substitution cipher with word divisions using non-pattern word lists*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1975. ISBN ???? 20 + 108 pp. LCCN Z103 .B3.

Barker:1977:CHC

[Bar77] Wayne G. Barker. *Cryptanalysis of the Hagelin cryptograph*, volume 17 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1977. ISBN 0-89412-022-0. xi + 223 pp. LCCN ????

Barker:1979:CEC

[Bar79a] Wayne G. Barker. *Cryptanalysis of an enciphered code problem: where an "additive" method of encipherment has been used*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1979. ISBN 0-89412-037-9. vii + 174 pp. LCCN Z103 .B333.

Barker:1979:HCCb

[Bar79b] Wayne G. Barker, editor. *The history of codes and ciphers in the United States during the period between the World Wars*, volume 22, 54 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1979. ISBN 0-89412-039-5 (part 1), 0-89412-165-0 (part 2). various pp. LCCN UB290 .H47 1979. Two volumes. This book was written about 1946 by the Historical Section of the Army Security Agency.

Barker:1979:HCCa

[Bar79c] Wayne G. Barker, editor. *The history of codes and ciphers in the United States during World War I*, volume 20 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1979. ISBN 0-89412-031-X. 263 pp. LCCN D639.C75 H57 1979.

Barker:1984:CSG

[Bar84] Wayne G. Barker. *Cryptanalysis of shift-register generated stream cipher systems*, volume 39 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1984. ISBN 0-89412-062-X. ix + 247 pp. LCCN Z 104 B37 1984.

Barrett:1987:IRS

[Bar87] Paul Barrett. Implementing the Rivest, Shamir and Adleman public-key encryption algorithm on a standard digital signal processor. In Odlyzko [Odl87b], pages 311–323. CODEN LNCSD9. ISBN

3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Barker:1991:IAD

[Bar91] Wayne G. Barker. *Introduction to the analysis of the Data Encryption Standard (DES)*, volume 55 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1991. ISBN 0-89412-169-3, 0-89412-170-7 (library). viii + 190 pp. LCCN QA76.9.A25B378 1991.

Barker:1992:CSC

[Bar92a] Wayne G. Barker. *Cryptanalysis of the single columnar transposition cipher*. Aegean Park Press, Laguna Hills, CA, USA, 1992. ISBN 0-89412-193-6. ix + 146 pp. LCCN ????

Barlow:1992:DPP

[Bar92b] John Perry Barlow. Decrypting the puzzle palace. *Communications of the Association for Computing Machinery*, 35(7):25–31, July 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/129910.html.

Barlow:1993:EFA

[Bar93a] John Perry Barlow. The electronic frontier: a plain text on crypto policy. *Communications of the Association for Computing Machinery*, 36(11):21–26, November 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/163378.html.

Barlow:1993:EFP

[Bar93b] John Perry Barlow. The electronic frontier: a plain text on crypto policy. *Communications of the Association for Computing Machinery*, 36(11):21–26, November 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/163378.html.

Barlow:1994:NSI

[Bar94] John Perry Barlow. *Notable Speeches of the Information Age*. 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, January 1994. ISBN 1-56592-992-6. LCCN ???? US$9.95. USENIX Conference Keynote Address, January 17, 1994; San Francisco, CA. Audio tape: 90 minutes.

Barker:1995:CDT

[Bar95] Wayne G. Barker. *Cryptanalysis of the double transposition cipher*, volume 69 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1995. ISBN 0-89412-069-7. v + 157 pp. LCCN ????

Barlas:1996:NKD

[Bar96a] Stephen Barlas. In the news: Key decisions likely on encryption exports. *IEEE Software*, 13(6):102–108, November 1996. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Barron:1996:RTR

[Bar96b] Nick Barron. *RSAEuro Technical Reference*. Compulink, ????, third edition, November 1996. v + 75 pp. URL http://www.rsaeuro.com/products/RSAEuro/rsadown.shtml; mailto:nikb@cix.compulink.co.uk.

Barias:1997:NBP

[Bar97] Stephen Barias. In the news: BSA pushes for override of encryption guidelines. *IEEE Software*, 14(2):136, March/April 1997. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Barnes:1999:ESJ

[Bar99] Darryl Barnes. Embedded systems: Java Card application development. *Dr. Dobb's Journal of Software Tools*, 24(2):72, 74, 76–78, 80, February 1999. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/1999/9902/9902toc.htm; http://www.ddj.com/ftp/1999/1999_02/jcard.txt.

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.

Baskerville:1993:ISS

[Bas93] Richard Baskerville. Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, 25(4):375–414, December 1993. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0360-0300/162127.html`.

Bastian:1995:CCE

[Bas95] Pat Bastian. Constitutional considerations of the Escrowed Encryption Standard, 1995. Paper presented to the Association for Education in Journalism and Mass Communication, Washington, DC, August, 1995.

Bassham:1998:ETA

[Bas98] Lawrence E. Bassham III. Efficiency testing of ANSI C implementations of Round1 candidate algorithms for the Advanced Encryption Standard. In National Institute of Standards and Technology [Nat98], page 30. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/r1-ansic.pdf`. See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

Baudouin:1939:ECF

[Bau39] Roger Baudouin. *Éléments de cryptographie. (French) [Elements of cryptography]*. A. Pedone, Paris, France, 1939. 336 pp.

Baudouin:1946:ECF

[Bau46] Roger Baudouin. *Éléments de cryptographie. (French) [Elements of cryptography]*. A. Pedone, Paris, France, 1946. 336 pp.

Bauer:1982:KVM

[Bau82] Friedrich L. Bauer. Kryptologie — Verfahren und Maximen. (German) [Cryptology — procedures and maxims]. *Informatik Spektrum*, 5(??):74–81, ???? 1982. CODEN INSKDW. ISSN 0170-6012 (print), 1432-122X (electronic).

Bauer:1997:DSM

[Bau97] Friedrich Ludwig Bauer. *Decrypted secrets: methods and maxims of cryptology*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. ISBN 3-540-60418-9. xii + 447 pp. LCCN QA76.9.A25 B38513 1997. With 166 figures, 26 tables and 16 color plates.

Baxter:1997:SBE

[Bax97] Mark Darrell Baxter. Selecting the best encryption system for the Defense Message System (DMS). Thesis (M.S.), University of Colorado, Boulder, CO, USA, 1997. xi + 121 pp.

Bowers:1960:PC

[BB60] William Maxwell Bowers and William G. Bryan. *Practical cryptanalysis*. American Cryptogram Association, Greenfield, MA, USA, 1960. ?? pp. LCCN Z103 .B6. Bound in printed paper wrappers. Contents: v. 1. Digraphic substitution; the playfair cypher, the four square cypher.– v. 2. The Bifid cipher. — v. 3. The Trifid cipher.– v. 4. Cryptographic ABC'S; Substitution and transposition ciphers, by William G. Bryan. — v. 5. Cryptographic ABC's; periodic ciphers, miscellaneous, by William G. Bryan.

Bowers:1967:PC

[BB67] William Maxwell Bowers and William G. Bryan. *Practical cryptanalysis*. American Cryptogrm Association, Greenfield, MA, USA, 1967. various pp.

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).

Bennett:1985:UQC

[BB85] Charles H. Bennett and Gilles Brassard. An update on quantum cryptography. In Blakley and Chaum [BC85], pages 475–480. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=475`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Bennett:1989:EQC

[BB89] C. H. Bennett and G. Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM SIGACT News*, 20(4):78–80, November 1989. CODEN SIGNDM. ISSN

0163-5700 (print), 1943-5827 (electronic).

Ben-Aroya:1994:DCL

[BB94] Ishai Ben-Aroya and Eli Biham. Differential cryptanalysis of Lucifer. *Lecture Notes in Computer Science*, 773:187–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1995:HSU

[BB95a] E. Biham and A. Biryukov. How to strengthen DES using existing hardware. *Lecture Notes in Computer Science*, 917:398–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1995:IDA

[BB95b] E. Biham and A. Biryukov. An improvement of Davies' attack on DES. *Lecture Notes in Computer Science*, 950:461–467, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blaze:1995:SLE

[BB95c] Matt Blaze and Steven M. Bellovin. Session-layer encryption. In USENIX Association [USE95b], pages 85–94 (or 85–93??). ISBN 1-880446-70-7. LCCN QA76.8.U65 U55 1992(3)-1995(5). URL http://www.usenix.org/publications/library/proceedings/security95/index.html.

Baum:1981:RPC

[BBB+81] Werner A. Baum, David H. Brandin, R. Creighton Buck, George I. Davida, George Handelman, Martin E. Hellman, Ira Michael Heyman, Wilfred Kaplan, and Daniel C. Schwartz. Report of the Public Cryptography Study Group, prepared for American Council on Education, One Dupont Circle, Washington, DC 20036, February 7, 1981. *Communications of the Association for Computing Machinery*, 24(7): 435–445, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See the opposing view in [Dav81].

Bennett:1991:EQC

[BBB+91] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Lecture Notes in Computer Science*, 473:253–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730253.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730253.pdf.

Barni:1998:MPI

[BBC98] M. Barni, F. Bartolini, and V. Cappellini. A M.A.P. identification criterion for DCT-based watermarking. In Theodoridis et al. [T+98], pages 17–20. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073107.html. Four volumes.

Blakley:1993:TSD

[BBCM93a] B. Blakley, G. R. Blakley, A. H. Chan, and J. L. Massey. Threshold schernes with disenrollment. *Lecture Notes in Computer Science*, 740:540–548, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blakley:1993:TPD

[BBCM93b] R. Blakley, G. R. Blakley, A. H. Chan, and J. L. Massey. Threshold protocols with disenrollment. In Brickell [Bri93], pages 540–548. CODEN LNCSD9. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1992. DM104.00.

Bennett:1995:GPA

[BBCM95] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, ???? 1995. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Barni:1997:RWS

[BBCP97] M. Barni, F. Bartolini, V. Cappellini, and A. Piva. Robust watermarking of still images for copyright protection. In IEEE [IEE97c], pages 499–502. ISBN 0-7803-4137-6 (softbound), 0-7803-4138-4 (microfiche), 0-7803-4139-2 (CDROM). LCCN TK5102.5.D448245 1997. Two volumes. IEEE catalog number 97TH8306.

Barni:1998:CPD

[BBCP98a] Mauro Barni, Franco Bartolini, Vito Cappellini, and Alessandro Piva. Copyright protection of digital images by embedded unperceivable marks. *Image and Vision Computing*, 16(12-13):897–906, August 1998. CODEN IVCODK. ISSN 0262-8856.

Barni:1998:DDS

[BBCP98b] Mauro Barni, Franco Bartolini, Vito Cappellini, and Alessandro Piva. A DCT-domain system for robust image watermarking. *Signal Processing*, 66(3):357–372, May 1998. CODEN SPRODR. ISSN 0165-1684. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073108.html.

Biguen:1997:ECM

[BBDF97] E. S. Biguen, J. Biguen, B. Duc, and S. Fischer. Expert conciliation for multi modal person authentication systems by Bayesian statistics. *Lecture Notes in Computer Science*, 1206: 291–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1999:IOS

[BBDR99] E. Biham, A. Biryukov, O. Dunkelman, and E. Richardson. Initial observations on Skipjack: Cryptanalysis of Skipjack-3XOR. *Lecture Notes in Computer Science*, 1556:362–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blackburn:1996:EMS

[BBDW96] S. R. Blackburn, M. Burmester, Y. Desmedt, and P. R. Wild. Efficient multiplicative sharing schemes. In Maurer [Mau96b], pages 107–118. CODEN LNCSD9. ISBN 3-540-61186-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1996. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1070.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1070. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Bennett:1992:QC

[BBE92] Charles H. Bennett, Gilles Brassard, and Artur K. Ekert. Quantum cryptography. *Scientific American*, 267(4):50–?? (Int. ed. 26–??), October 1992. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Bauer:1983:KDP

[BBF83] R. K. Bauer, T. A. Berson, and R. J. Feiertag. A key distribution protocol using event markers. *ACM Transactions on Computer Systems*, 1(3):249–255, August 1983. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Biham:1998:CM

[BBF+98] E. Biham, A. Biryukov, Niels Ferguson, Lars R. Knudsen, Bruce Schneier, and Adi Shamir. Cryptanalysis of Magenta. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, August 20, 1998. URL `http://www.counterpane.com/magenta.html`.

Bertilsson:1990:CVE

[BBI90] Michael Bertilsson, Ernest F. Brickell, and Ingemar Ingemarsson. Cryptanalysis of video encryption based on space-filling curves. In Quisquater and Vandewalle [QV90], pages 403–411. CODEN LNCSD9. ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1989; QA267.A1 L43 no.434. DM98.00. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340403.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340403.pdf`.

Bleichenbacher:1995:SRL

[BBL95] Daniel Bleichenbacher, Wieb Bosma, and Arjen K. Lenstra. Some remarks on Lucas-based cryptosystems. *Lecture Notes in Computer Science*, 963:386–396, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Benantar:1996:AOS

[BBN96] M. Benantar, B. Blakley, and A. J. Nadalin. Approach to object security in Distributed SOM. *IBM Systems Journal*, 35 (2):192–203, 1996. CODEN IBMSA7. ISSN 0018-8670. URL `http://www.research.ibm.com/journal/sj35-2.html#six`.

Boyar:1995:SZ

[BBP95a] Joan Boyar, Gilles Brassard, and René Peralta. Subquadratic zero-knowledge. *Journal of the Association for Computing Machinery*, 42(6):1169–1193, November 1995. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/227686.html`.

Boyar:1995:SZK

[BBP95b] Joan Boyar, Gilles Brassard, and René Peralta. Subquadratic zero-knowledge. *Journal of the Association for Computing Machinery*, 42(6):1169–1193, November 1995. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/227686.html`.

Bennett:1988:PAP

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Biham:1999:BGD

[BBR99] Eli Biham, Dan Boneh, and Omer Reingold. Breaking generalized Diffie–Hellman modulo a composite is no easier than factoring. *Information Processing Letters*, 70(2):83–87, April 30, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Biham:1998:CSR

[BBS98a] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. Technical report 0947, Department of Computer Science, Technion — Israel Institute of Technology, Haifa, Israel, 1998. 12 pp.

Blaze:1998:DPA

[BBS98b] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. *Lecture Notes in Computer Science*, 1403:127–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1999:CSR

[BBS99a] E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. *Lecture Notes in Computer Science*, 1592:12–23, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1999:MMA

[BBS99b] E. Biham, A. Biryukov, and A. Shamir. Miss in the middle attacks on IDEA and Khufu. In Knudsen [Knu99c], pages 124–138. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Biehl:1994:CPB

[BBT94] Ingrid Biehl, Johannes A. Buchmann, and Christoph Thiel. Cryptographic protocols based on discrete logarithms in real-quadratic orders. In Desmedt [Des94b], pages 56–60. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390056.`

htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390056.pdf.

Blakley:1985:ACP

[BC85] George Robert Blakley and David Chaum, editors. *Advances in Cryptology: Proceedings of CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0196.htm; http://www.springerlink.com/content/cemajg0qmeev/; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=196. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Bender:1990:IEC

[BC90] Andreas Bender and Guy Castagnoli. On the implementation of elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 435:186–192, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beimel:1993:UIS

[BC93a] Amos Beimel and Benny Chor. Universally ideal secret sharing schemes (preliminary version). *Lecture Notes in Computer Science*, 740:183–195, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0740/07400183.htm; http://link.springer-ny.com/link/service/series/0558/papers/0740/07400183.pdf.

Bos:1993:PUS

[BC93b] J. N. E. Bos and D. Chaum. Provably unforgeable signatures. *Lecture Notes in Computer Science*, 740:1–14, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beguin:1995:GSC

[BC95a] P. Beguin and A. Cresti. General short computational secret sharing schemes. *Lecture Notes in Computer Science*, 921:194–??, 1995. CODEN LNCSD9. ISSN

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

Beimel:1995:SSP

[BC95b] A. Beimel and B. Chor. Secret sharing with public reconstruction. *Lecture Notes in Computer Science*, 963:353–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1995:SRB

[BC95c] Carlo Blundo and Antonella Cresti. Space requirements for broadcast encryption. *Lecture Notes in Computer Science*, 950: 287–298, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500287.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0950/09500287.pdf`.

Blundo:1996:BES

[BC96a] Carlo Blundo and Antonella Cresti. Broadcast encryption schemes with disenrollment capability. In *Theoretical computer science (Ravello, 1995)*, pages 176–191. World Scientific Publishing Co., Singapore; Philadelphia, PA, USA; River Edge, NJ, USA, 1996.

Brassard:1996:YQC

[BC96b] Gilles Brassard and Claude Crépeau. 25 years of quantum cryptography. *ACM SIGACT News*, 27(3):13–24, September 1996. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Baldwin:1997:LS

[BC97] R. W. Baldwin and C. V. Chang. Locking the e-safe. *IEEE Spectrum*, 34(2):40–46, February 1997. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Blakley:1998:C

[BC98] G. R. Blakley and D. Chaum. Crypto '84. *Lecture Notes in Computer Science*, 1440: 35–40, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Burwick:1998:MCC

[BCA+98] C. Burwick, D. Coppersmith, E. D. Avignon, R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas Jr., L. O. Connor, M. Peyravian, D. Safford, and N. Zunic. MARS — a candidate cipher for AES. NIST AES Proposal, June 1998.

Barker:1988:ECT

[BCB88] W. C. Barker, P. Cochrane, and M. Branstad. Embedding cryptography into a Trusted Mach system. In IEEE [IEE88], pages 379–383. ISBN 0-8186-0895-1. LCCN TL787 .A471 1988; QA76.9.A25 A39 1988. IEEE catalog number 88CH2629-5. IEEE Computer Society order number 895.

Bigun:1997:AVB

[BCB97] Josef Bigun, Gerard Chollet, and Gunilla. Borgefors, editors. *Audio- and video-based biometric person authentication: First International Conference, AVBPA '97, Crans-Montana, Switzerland, March 12–14, 1997: proceedings*, volume 1206 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-62660-3 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7882.S65 A944 1997. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1206.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1206.

Blair:1999:DRA

[BCCD99] G. S. Blair, F. Costa, G. Coulson, and H. Duran. The design of a resource-aware reflective middleware architecture. *Lecture Notes in Computer Science*, 1616: 115–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Baritaud:1993:SPK

[BCCG93] T. Baritaud, M. Campana, P. Chauvaud, and H. Gilbert. On the security of the permuted kernel identification scheme. *Lecture Notes in Computer Science*, 740:305–311, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brucoli:1999:DHC

[BCCG99] Michele Brucoli, Donato Cafagna, Leonarda Carnimeo, and Giuseppe Grassi. Design of a hyperchaotic cryptosystem based on identical and generalized synchronization. *International journal of bifurcation and chaos in applied sciences and engineering*, 9 (10):2027–2037, 1999. CODEN IJBEE4. ISSN 0218-1274.

Bas:1998:SSB

[BCD98] P. Bas, J. M. Chassery, and F. Davoine. Self-similarity based image watermarking. In Theodoridis et al. [T+98], pages 2277–2280. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN

TK5102.9.E97 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073109.html. Four volumes.

Boyar:1991:CUS

[BCDP91] J. Boyar, D. Chaum, I. Damgård, and T. Pederson. Convertible undeniable signatures. In Menezes and Vanstone [MV91], pages 189–205. CODEN LNCSD9. ISBN 0-387-54508-5 (New York), 3-540-54508-5 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1990. Conference held Aug. 11–15, 1990, at the University of California, Santa Barbara.

Blundo:1994:FDS

[BCDV94] C. Blundo, A. Cresti, A. De Santis, and U. Vaccaro. Fully dynamic secret sharing schemes. *Lecture Notes in Computer Science*, 773: 110–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1996:FDS

[BCDV96] Carlo Blundo, Antonella Cresti, Alfredo De Santis, and Ugo Vaccaro. Fully dynamic secret sharing schemes. *Theoretical Computer Science*, 165(2):407–440, October 10, 1996. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1996&volume=165&issue=2&aid=2206.

Barkee:1994:WYC

[BCE+94] Boo Barkee, Deh Cac Can, Julia Ecks, Theo Moriarty, and R. F. Ree. Why you cannot even hope to use Gröbner bases in public key cryptography: An open letter to a scientist who failed and a challenge to those who have not yet failed. *Journal of Symbolic Computation*, 18 (6):497–502 (or 497–501??), December 1994. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Bellare:1990:SSK

[BCG90] Mihir Bellare, Lenore Cowen, and Shafi Goldwasser. On the structure of secret key exchange protocols. *Lecture Notes in Computer Science*, 435:604–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350604.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350604.pdf.

Beth:1985:ACP

[BCI85] Thomas Beth, N. Cot, and I. Ingemarsson, editors. *Advances in cryptology: proceedings of EUROCRYPT 84, a Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, April 9–11, 1984*, volume 209 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0209.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=209`. Held at the University of Paris, Sorbonne.

Beth:1998:Eb

[BCI98] T. Beth, N. Cot, and I. Ingemarsson. Eurocrypt '84. *Lecture Notes in Computer Science*, 1440:29–34, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1996:HC

[BCK96a] M. Bellare, R. Canetti, and H. Krawczyk. The HMAC construction. *CryptoBytes*, 2(1):12–15, 1996.

Bellare:1996:PFRa

[BCK96b] M. Bellare, R. Canetti, and H. Krawczyk. Pseudorandom functions revisited: The cascade construction. Manuscript., April 1996.

Bellare:1996:PFRb

[BCK96c] M. Bellare, R. Canetti, and H. Krawczyk. Pseudorandom functions revisited: the cascade construction and its concrete security. In IEEE [IEE96a], pages 514–523. CODEN ASFPDV. ISBN 0-7803-3762-X (casebound), 0-8186-7594-2 (softbound), 0-8186-7596-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1996. IEEE catalog number 96CH35973. IEEE Computer Society Press order number PR07594.

Bellare:1996:KHF

[BCK96d] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In Koblitz [Kob96], pages 1–15. CODEN LNCSD9. ISBN 3-540-61512-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1996. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090001.htm; http://link.springer-`

ny.com/link/service/series/0558/papers/1109/11090001.pdf; http://www.research.ibm.com/security/. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Bellare:1996:MAU

[BCK96e] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Message authentication using hash functions: the HMAC construction. *CryptoBytes*, 2(1):12–15, Spring 1996. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n1.pdf.

Bellare:1998:MAD

[BCK98] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract). In ACM [ACM98b], pages 419–428. ISBN 0-89791-962-9. LCCN QA75.5 .A14 1998. URL http://www.acm.org/pubs/articles/proceedings/stoc/276698/p419-bellare/p419-bellare.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/276698/p419-bellare/. ACM order number 508980.

Bellare:19xx:KMM

[BCKxx] M. Bellare, R. Canetti, and H. Krawczyk. Keying MD5 — message authentication via iterated pseudorandomness. In preparation., 19xx.

Bromley:1983:RFM

[BCKS+83] Allan G. Bromley, Martin Campbell-Kelly, K. W. Smillie, Eric A. Weiss, Saul Rosen, and Cipher A. Deavours. Reviews: O. I. Franksen: Mr. Babbage, the Difference Engine, and the Problem of Notation: An Account of the Origin of Recursiveness and Conditionals in Computer Programming; H. Lukoff: from Dits to Bits; I. Asimov: Asimov's Biographical Encyclopedia of Science and Technology; J. Futrelle: Thinking Machine; R. M. Hord: The Illiac IV; C. H. Meyer and S. M. Matyas: Cryptography; T. J. Peters and R. H. Waterman: In Search of Excellence; J. W. Stokes: 70 Years of Radio Tubes and Valves; G. Welchman: The Hut Six Story; capsule reviews. *Annals of the History of Computing*, 5(4):411–427, October/December 1983. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/

an1983/pdf/a4411.pdf; http://www.computer.org/annals/an1983/a4411abs.htm.

Bergadano:1998:HDC

[BCR98] Francesco Bergadano, Bruno Crispo, and Giancarlo Ruffo. High dictionary compression for proactive password checking. *ACM Transactions on Information and System Security*, 1(1):3–25, November 1998. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org:80/pubs/citations/journals/tissec/1998-1-1/p3-bergadano/.

Berbecel:1997:MTW

[BCV97] Gh. Berbecel, T. Cooklev, and A. N. Venetsanopoulos. Multiresolution technique for watermarking digital images. In IEEE [IEE97g], pages 354–355. CODEN DTPEEL. ISBN 0-7803-3735-2 (casebound), 0-7803-3734-4 (paperback), 0-7803-3736-0 (microfiche). ISSN 0747-668X. LCCN ????

Birnbaum:1986:VPS

[BCW86] Martha Birnbaum, Larry A. Cohen, and Frank X. Welsh. Voice password system for access security. *AT&T Technical Journal*, 65(5):68–74, September 1986. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Bishop:1997:TNI

[BCW97] M. Bishop, S. Cheung, and C. Wee. The threat from the net [Internet security]. *IEEE Spectrum*, 34(8):56–63, August 1997. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Borucki:1974:MNN

[BD74] L. J. Borucki and J. B. Diaz. Mathematical notes: a note on primes, with arbitrary initial or terminal decimal ciphers, in Dirichlet arithmetic progressions. *American Mathematical Monthly*, 81(9):1001–1002, November 1974. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Brickell:1990:CIS

[BD90] Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes (extended abstract). *Lecture Notes in Computer Science*, 435:278–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350278.htm; http://link.springer-ny.com/link/service/series/

0558/papers/0435/04350278.pdf.

Burmester:1991:ALN

[BD91] Mike V. D. Burmester and Yvo Desmedt. All languages in NP have divertible zero-knowledge proofs and arguments under cryptographic assumptions (extended abstract). *Lecture Notes in Computer Science*, 473:1–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730001.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730001.pdf.

Bauspiess:1992:RCH

[BD92] Fritz Bauspiess and Frank Damm. Requirements for cryptographic hash functions. *Computers and Security*, 11(5):427–437, September 1, 1992. CODEN CPSEDU. ISSN 0167-4048.

Brandt:1993:GPP

[BD93] J. Brandt and I. Damgaard. On generation of probable primes by incremental search. *Lecture Notes in Computer Science*, 740:358–370, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bloecher:1994:FFS

[BD94] U. Bloecher and M. Dichtl. Fish: a fast software stream cipher. *Lecture Notes in Computer Science*, 809:41–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bloecher:1995:PLC

[BD95a] U. Bloecher and M. Dichtl. Problems with the linear cryptanalysis of DES using more than one active S-box per round. *Lecture Notes in Computer Science*, 1008:265–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Burmester:1995:SEC

[BD95b] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. *Lecture Notes in Computer Science*, 950:275–286, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1997:LBR

[BD97] Carlo Blundo and Alfredo De Santis. Lower bounds for robust secret sharing schemes. *Information Processing Letters*, 63(6):317–321, October 8, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Bao:1998:SSS

[BD98a] Feng Bao and Robert H. Deng. A signcryption scheme with signature directly verifiable by public key. *Lecture Notes in Computer Science*, 1431: 55–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310055.htm; http://link.springer-ny.com/link/service/series/0558/papers/1431/14310055.pdf.

Blundo:1998:VCS

[BD98b] Carlo Blundo and Alfredo De Santis. Visual cryptography schemes with perfect reconstruction of black pixels. *Computers and Graphics*, 22(4):449–455, August 1, 1998. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.elsevier.com/cas/tree/store/cag/sub/1998/22/4/568.pdf.

Bao:1999:NTM

[BD99a] F. Bao and R. H. Deng. A new type of "magic ink" signatures — towards transcript-irrelevant anonymity revocation. *Lecture Notes in Computer Science*, 1560:1–11, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boneh:1999:CRP

[BD99b] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *Lecture Notes in Computer Science*, 1592:1–11, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1592/15920001.pdf.

Burmester:1992:EZK

[BDB92] M. V. D. Burmester, Y. G. Desmedt, and T. Beth. Efficient zero-knowledge identification schemes for smart cards. *The Computer Journal*, 35(1):21–29, February 1992. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/Volume_35/Issue_01/Vol35_01.body.html#AbstractBurmester.

Branwyn:1995:IRA

[BDC+95] Gareth Branwyn, Luke Duncan, Sean Carton, Donald Rose, Tom Lichty, Shannon R. Turlingon, and Jan Weingarten. *Internet* *roadside attractions: sites, sounds and scenes along the information superhighway*. Ventana Press, Chapel Hill, NC, USA, 1995. ISBN 1-56604-193-7. xxxiv + 320 pp. LCCN TK5105.875.I57 I573 1995.

Blundo:1994:MSS

[BDD+94] Carlo Blundo, Alfredo De Santis, Giovanni Di Crescenzo, Antonio Giorgio Gaggia, and Ugo Vaccaro. Multi-secret sharing schemes. In Desmedt [Des94b], pages 150–163. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390150.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390150.pdf.

Bondalapati:1999:DDE

[BDDG99] K. Bondalapati, P. Diniz, P. Duncan, and J. Granacki. DEFACTO: a design environment for adaptive computing technology. *Lecture Notes in Computer Science*, 1586:570–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boneh:1998:ARG

[BDF98] D. Boneh, G. Durfee, and Y. Frankel. An attack on RSA given a small fraction of the private key bits. *Lecture Notes in Computer Science*, 1514:25–34, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://theory.stanford.edu/~dabo/papers/bits_of_d.ps.

BenAyed:1999:MFP

[BDFM99] R. Ben Ayed, J. Desharnais, M. Frappier, and A. Mill. Mathematical foundations for program transformations. *Lecture Notes in Computer Science*, 1559: 319–321, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1999:PSS

[BDG99] C. Blundo, A. De Santis, and A. Giorgio Gaggia. Probability of shares in secret sharing schemes. *Information Processing Letters*, 72(5–6):169–175, December 30, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.nl/gej-ng/10/23/20/60/25/28/abstract.html; http://www.elsevier.nl/gej-ng/10/23/20/60/25/28/article.pdf.

Bao:1998:MFA

[BDGI98] F. Bao, R. H. Deng, X. Gao, and Y. Igarashi. Modified finite automata public key cryptosystem. *Lecture Notes in Computer Science*, 1396:82–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1993:IRS

[BDGV93] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes. *Lecture Notes in Computer Science*, 740: 148–167, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1996:IRS

[BDGV96] Carlo Blundo, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the information rate of secret sharing schemes. *Theoretical Computer Science*, 154(2):283–306, February 05, 1996. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1996&volume=154&issue=2&aid=2003`.

Boneh:1999:FL

[BDHG99a] D. Boneh, G. Durfee, and N. Howgrave-Graham. Factoring $N = p^r q$ for large r. *Lecture Notes in Computer Science*, 1666: 326–337, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boneh:1999:FPL

[BDHG99b] D. Boneh, G. Durfee, and N. Howgrave-Graham. Factoring $N = p^r q$ for large r. In Wiener [Wie99], pages 326–337. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Bao:1997:DAT

[BDHJ97] F. Bao, R. Deng, Y. Han, and A. Jeng. Design and analyses of two basic protocols for use in TTP-based key escrow. *Lecture Notes in Computer Science*, 1270: 261–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bao:1998:BPK

[BDHJ98] F. Bao, R. H. Deng, Y. F. Han, and A. B. R. Jeng. Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults. *Lecture Notes in Computer Science*, 1361:115–??, 1998. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Blundo:1993:PSK

[BDHK93] C. Blundo, A. De Santis, A. Herzberg, and S. Kutten. Perfectly-secure key distribution for dynamic conferences. *Lecture Notes in Computer Science*, 740: 471–486, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Burmester:1996:PRS

[BDI+96] M. Burmester, Y. G. Desmedt, T. Itoh, K. Sakurai, H. Shizuya, and M. Yung. A progress report on subliminal-free channels. In Anderson [And96c], pages 157–168. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054604.html.

Bellare:1997:CST

[BDJR97] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In IEEE [IEE97f], pages 394–403. CODEN ASFPDV. ISBN 0-8186-8197-7 (paperback), 0-8186-8198-5 (casebound), 0-8186-8199-3 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 .S92 1997. IEEE catalog number 97CB36150. IEEE Computer Society Press order number PR08197.

Boneh:1997:ICC

[BDL97] D. Boneh, R. A. Demillo, and R. J. Lipton. On the importance of checking cryptographic protocols for faults. *Lecture Notes in Computer Science*, 1233:37–51, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://theory.stanford.edu/~dabo/papers/faults.ps.gz.

Benaloh:1994:OWA

[BdM94] Josh Cohen Benaloh and Michael de Mare. One-way accumulators: a decentralized alternative to digital signatures. *Lecture Notes in Computer Science*, 765:274–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650274.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650274.pdf.

Bosselaers:1997:RCH

[BDP97] Antoon Bosselaers, Hans Dogbbertin, and Bart Preneel. The RIPEMD-160 cryptographic hash function. *Dr. Dobb's Journal of Software Tools*, 22(1):24, 26, 28, 78, 80, January 1997. CODEN DDJOEB. ISSN 1044-789X.

Bellare:1998:RAN

[BDPR98] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. *Lecture Notes in Computer Science*, 1462:26–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620026.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620026.pdf.

Baraani-Dastjerdi:1995:CMO

[BDPSNG95] A. Baraani-Dastjerdi, J. Pieprzyk, R. Safavi-Naini, and J. Getta. A cryptographic mechanism for object-instance-based authorization in object-oriented database systems. *Lecture Notes in Computer Science*, 1021:44–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Baraani-Dastjerdi:1997:UCH

[BDPSNG97] A. Baraani-Dastjerdi, J. Pieprzyk, R. Safavi-Naini, and J. R. Getta. Using cryptographic hash functions for discretionary access control in object-oriented databases. *J.UCS: Journal of Universal Computer Science*, 3(6):730–??, June 28, 1997. ISSN 0948-6968. URL http://medoc.springer.de:8000/jucs_3_6/using_cryptographic_functions_for; internal&sk=05460486.

Blaze:1996:MKL

[BDR+96] M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner. Minimal key lengths for symmetric ciphers to provide adequate commercial security. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, January 1996. URL http://www.bsa.org/policy/encryption/cryptographers.html; http://www.counterpane.com/keylength.html.

Burmester:1998:EKE

[BDS98] M. Burmester, Y. Desmedt, and J. Seberry. Equitable key escrow with limited time span (or how to enforce time expiration cryptographically). *Lecture Notes in Computer Science*, 1514:380–??, 1998. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Blundo:1993:GDS

[BDSV93] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *Lecture Notes in Computer Science*, 658:1–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1993:ESM

[BDV93] C. Blundo, A. De Santis, and U. Vaccaro. Efficient sharing of many secrets. *Lecture Notes in Computer Science*, 665:692–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1998:SSS

[BDV98] Carlo Blundo, Alfredo De Santis, and Ugo Vaccaro. On secret sharing schemes. *Information Processing Letters*, 65(1):25–32, January 15, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Bright:1976:CUM

[BE76] H. S. Bright and R. L. Enison. Cryptography using modular software elements. *AFIPS Conference Proceedings*, 45(??):113–123, ???? 1976.

Bright:1979:QRN

[BE79] Herbert S. Bright and Richard L. Enison. Quasi-random number sequences from a long-period TLP generator with remarks on application to cryptography. *ACM Computing Surveys*, 11(4):357–370, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Barrett:1990:SDU

[BE90] Paul Barrett and Raymund Eisele. The smart diskette — a universal user token and personal crypto-engine (invited). *Lecture Notes in Computer Science*, 435:74–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350074.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350074.pdf`.

Beardsley:1972:YCI

[Bea72] C. W. Beardsley. Is your computer insecure? *IEEE Spectrum*, 9(1):67–78, January 1972. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Beauquier:1992:TDP

[Bea92] J. Beauquier. Two distributed problems involving

Byzantine processes. *Theoretical Computer Science*, 95(1):169–185, March 23, 1992. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Beaver:1993:HBS

[Bea93] D. Beaver. How to break a "secure" oblivious transfer protocol. *Lecture Notes in Computer Science*, 658: 285–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beaver:1996:ASE

[Bea96] Donald Beaver. Adaptively secure encryption. Technical report CSE-96-031, Department of Computer Science and Engineering, College of Engineering, Pennsylvania State University, University Park, PA, USA, February 1996. 15 pp.

Beaver:1997:CBC

[Bea97a] Donald Beaver. Commodity-based cryptography (extended abstract). In ACM [ACM97c], pages 446–455. ISBN 0-89791-888-6. LCCN QA76.5 .A849 1997. URL http://www.acm.org/pubs/articles/proceedings/stoc/258533/p446-beaver/p446-beaver.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/258533/p446-beaver/. ACM order no. 508970.

Beaver:1997:PPE

[Bea97b] Donald Beaver. Plug and play encryption. *Lecture Notes in Computer Science*, 1294:75–89, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940075.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940075.pdf.

Becker:1982:EDE

[Bec82] Michael S. Becker. An exercise with the Data Encryption Standard. Master of science, plan ii, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA, 1982. 56 pp.

Beckett:1988:IC

[Bec88] Brian Beckett. *Introduction to cryptology*. Professional and industrial computing series. Blackwell Scientific Publications, Oxford, UK, 1988. ISBN 0-632-01836-4 (paperback), 0-632-02243-4. xiv + 344 pp. LCCN QA76.9.A25 B43 1988.

Beckett:1990:IAM

[Bec90] Brian Beckett. *Introduction aux méthodes de la cryptologie*, volume 5 of

Logique mathematiques informatique. Masson Editeur, Masson, France, 1990. ISBN 2-225-81941-6. 332 pp. LCCN ????

Beckett:1997:ICP

[Bec97] Brian Beckett. *Introduction to cryptolology and PC security*. McGraw-Hill, New York, NY, USA, 1997. ISBN 0-07-709235-X (hardback). viii + 356 pp. LCCN QA76.9.A25 B43 1997. Updated edition of *Introduction to cryptology* [Bec88].

Beck:1999:DPE

[Bec99] Robert Beck. Dealing with public Ethernet jacks — switches, gateways, and authentication. In USENIX [USE99b], page ?? ISBN 1-880446-25-1. LCCN ???? URL `http://db.usenix.org/publications/library/proceedings/lisa99/beck.html`.

Bedini:1990:TJS

[Bed90] Silvio A. Bedini. *Thomas Jefferson: statesman of science*. MacMillan Publishing Company, New York, NY, USA, 1990. ISBN 0-02-897041-1. xviii + 616 + 24 pp. LCCN E332.2 .B37 1990.

Beesly:1981:CIW

[Bee81] Patrick Beesly. *Cryptanalysis and its influence on the war at sea 1914–1918*. U.S. Naval Academy, Annapolis, MD, USA, 1981. 13 pp.

Bee:1996:UGA

[Bee96] Andrianne Bee. US government allows selling of strong encryption to US clients. *Network Security*, 1996(9): 6, September 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/1353485896844035`.

Bee:1997:LE

[Bee97] Adrianne Bee. The latest on encryption. *Network Security*, 1997(2):6–7, February 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485897866469`.

Behrens:1954:EUP

[Beh54] Carl E. Behrens. Effects on U-boat performance of intelligence from decryption of Allied communication. Technical report OEG study 553, Distributed by NTIS, Springfield, VA, USA, 1954. various pp.

Bell:1977:IVU

[Bel77] Ernest L. Bell. *An initial view of Ultra as an American weapon*. T S U Press, Keene, NH, USA, 1977. iii

+ 110 pp. LCCN D810.C88 B45.

Bellcore:1992:GRX

[Bel92] Bellcore. Generic requirements for X Window System security. Technical Report FA-STS-991324, Framework Technical Advisory, June 30 1992. Describes some of the problems associated with X in a commercial environment, and specifies solutions including Kerberos. Also talks about auditing in X.

Bellovin:1998:CI

[Bel98] S. M. Bellovin. Cryptography and the Internet. *Lecture Notes in Computer Science*, 1462:46–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1999:POP

[Bel99] M. Bellare. Practice-oriented provable security. *Lecture Notes in Computer Science*, 1561:1–15, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bennett:1980:UWN

[Ben80] Ralph Francis Bennett. *Ultra in the West: the Normandy campaign, 1944–45*. Scribner, New York, NY, USA, 1980. ISBN 0-684-16704-2. xvi + 336 pp. LCCN D756.5.N6 B44 1980. US$17.50.

Bennett:1988:AEA

[Ben88] John Bennett. Analysis of the encryption algorithm used in the WordPerfect word processing program. *Computers and Security*, 7(1):105, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888905366`.

Bennett:1989:UMS

[Ben89] Ralph Francis Bennett. *Ultra and Mediterranean strategy 1941–1945*. H. Hamilton, London, UK, 1989. ISBN 0-241-12687-8. 496 pp. LCCN D766 .B46x 1989b.

Benario:1998:TSU

[Ben98] Janice M. Benario. Top secret ultra. *The Classical Bulletin*, 74(1):31–33, ???? 1998. ISSN 0009-8337.

Benedens:1999:GBW

[Ben99] Oliver Benedens. Geometry-based watermarking of 3D models. *IEEE Computer Graphics and Applications*, 19(1):46–55, January/February 1999. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic). URL `http://computer.org/cga/cg1999/g1046abs.htm`; `http://dlib.computer.org/cg/`

books/cg1999/pdf/g1046.pdf.

Bertrand:1973:EOP

[Ber73] Gustave Bertrand. *Enigma; ou, La plus grande énigme de la guerre 1939–1945*. Plon, Paris, France, 1973. 295 + 2 + 16 pp. LCCN ????

Berstis:1980:SPD

[Ber80] Viktors Berstis. Security and protection of data in the IBM System/38. *ACM SIGARCH Computer Architecture News*, 8(3): 245–252, 1980. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Bertrand:1983:EGE

[Ber83] Gustave Bertrand. *Enigma, or, The greatest enigma of the 1939–1945 war*. ????, ????, 1983. vi + 415 pp. LCCN ???? English translation by Russell Babcock Holmes of [Ber73].

Berkovits:1991:HBS

[Ber91] S. Berkovits. How to broadcast a secret. *Lecture Notes in Computer Science*, 547: 535–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Berson:1993:DCA

[Ber93] T. Berson. Differential cryptanalysis mod 2^32 with applications to MD5. In Rueppel [Rue93], pages 71–80. CODEN LNCSD9. ISBN 0-387-56413-6 (New York), 3-540-56413-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1992.

Berson:1996:HMO

[Ber96a] T. Berson. Her Majesty's Orthography Service. In Anderson [And96c], pages 345–346. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054310.html.

Berson:1996:NIC

[Ber96b] Thomas A. Berson. At the Newton Institute: Coding theory, cryptology, and computer security. *CryptoBytes*, 2(2):13–15, Summer 1996. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n2.pdf.

Berg:1997:JQHh

[Ber97a] Cliff Berg. Java Q and A: How do I create a signed applet? *Dr. Dobb's Journal of Software Tools*, 22(8): 109–111, 122, August 1997. CODEN DDJOEB. ISSN 1044-789X.

Berghel:1997:DVW

[Ber97b] Hal Berghel. Digital village — watermarking cyberspace. *Communications of the Association for Computing Machinery*, 40(11): 19–24, November 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org:80/pubs/citations/journals/cacm/1997-40-11/p19-berghel/.

Berson:1997:FMP

[Ber97c] Thomas A. Berson. Failure of the McEliece public-key cryptosystem under message-resend and related-message attack. *Lecture Notes in Computer Science*, 1294:213–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940213.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940213.pdf.

Berg:1998:JQHd

[Ber98] Cliff Berg. Java Q&A: How do I password encrypt data? *Dr. Dobb's Journal of Software Tools*, 23(8):107–109, 117, August 1998. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ftp/1998/1998_08/jqa898.txt; http://www.ddj.com/ftp/1998/1998_08/jqa898.zip.

Bergmann:2009:DKR

[Ber09] 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).

Beth:1983:CPW

[Bet83] Thomas Beth, editor. *Cryptography: proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, March 29–April 2, 1982*, volume 149 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1983. CODEN LNCSD9. ISBN 0-387-11993-0 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN Z102.5 .C78 1983. DM43.00.

Betts:1988:ESG

[Bet88] Mitch Betts. Encryption standard to get reprieve. *Computers and Security*, 7(1):106, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.

com/science/article/pii/0167404888905470.

Beth:1995:CCIb

[Bet95a] T. Beth. Confidential communication on the Internet. *Scientific American [International Edition]*, 273 (6):70–73, December 1995. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Beth:1995:CCIa

[Bet95b] Thomas Beth. Confidential communication on the Internet. *Scientific American*, 273(6):88–91 (Intl. ed. 70–73), December 1995. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Beth:1995:MST

[Bet95c] Thomas Beth. Multifeature security through homomorphic encryption. *Lecture Notes in Computer Science*, 917:3–17, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beth:1998:Ea

[Bet98] T. Beth. Eurocrypt '82. *Lecture Notes in Computer Science*, 1440:9–12, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beutelspacher:1994:CIA

[Beu94] Albrecht Beutelspacher. *Cryptology: an introduction to the art and science of enciphering, encrypting, concealing, hiding, and safeguarding described without any arcane skullduggery but not without cunning waggery for the delectation and instruction of the general public*. Spectrum series. Mathematical Association of America, Washington, DC, USA, 1994. ISBN 0-88385-504-6. xvi + 156 pp. LCCN Z 103 B4813 1994. Cryptology was originally published in German by Vieweg. This edition has been extensively revised.

Blaze:1996:MKC

[BF96] Matt Blaze and Joan Feigenbaum. Master-key cryptosystems. Technical Report TR-96-02, DIMACS, Center for Discrete Mathematics and Theoretical Computer Science, Rutgers, NJ, USA, 1996.

Beimel:1997:RCP

[BF97a] A. Beimel and M. Franklin. Reliable communication over partially authenticated networks. *Lecture Notes in Computer Science*, 1320: 245–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boneh:1997:EGS

[BF97b] Dan Boneh and Matthew Franklin. Efficient generation of shared RSA keys. *Lecture Notes in Computer Science*, 1294: 425–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940425.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940425.pdf.

Balfanz:1999:HHC

[BF99a] Dirk Balfanz and Edward W. Felten. Handheld computers can be better Smart Cards. In USENIX [USE99a], page ?? ISBN 1-880446-28-6. LCCN QA76.9.A25 U83 1999. URL http://db.usenix.org/publications/library/proceedings/sec99/balfanz.html.

Beimel:1999:RCP

[BF99b] Amos Beimel and Matthew Franklin. Reliable communication over partially authenticated networks. *Theoretical Computer Science*, 220(1):185–210, June 06, 1999. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cas/tree/store/tcs/sub/1999/220/1/3051.pdf.

Boneh:1999:EPK

[BF99c] Dan Boneh and Matthew Franklin. An efficient public key traitor tracing scheme. In Wiener [Wie99], pages 338–353. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660338.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660338.pdf.

Boneh:19xx:

[BFAFxx] D. Boneh, Ed Felten, Bill Aiello, and Matt Franklin. ???? ????, 19xx. URL http://gump.bellcore.com:7700.

Blaze:1999:KTM

[BFK99] Matt Blaze, Joan Feigenbaum, and Angelos D. Keromytis. KeyNote: Trust management for public-key infrastructures (position paper). *Lecture Notes in Computer Science*, 1550: 59–63, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1550/15500059.htm; http://link.springer-

ny.com/link/service/series/0558/papers/1550/15500059.pdf.

Blum:1994:CPB

[BFKL94] Avrim Blum, Merrick Furst, Michael Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. *Lecture Notes in Computer Science*, 773:278–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blum:1988:NIZ

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In ACM [ACM88], pages 103–112. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. URL http://www.acm.org/pubs/articles/proceedings/stoc/62212/p103-blum/p103-blum.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/62212/p103-blum/. ACM order no. 508880.

Blaze:1998:PSS

[BFN98a] M. Blaze, J. Feigenbaum, and M. Naor. Paradigms for symmetric systems: a formal treatment of remotely keyed encryption. *Lecture Notes in Computer Science*, 1403:251–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blaze:1998:FTR

[BFN98b] Matt Blaze, Joan Feigenbaum, and Moni Naor. A formal treatment of remotely keyed encryption (extended abstract). *Lecture Notes in Computer Science*, 1403:251–265, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030251.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030251.pdf.

Boyd:1999:EEC

[BFP99] C. Boyd, E. Foo, and C. Pavlovski. Efficient electronic cash using batch signatures. *Lecture Notes in Computer Science*, 1587:244–257, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beth:1992:PCS

[BFS92a] Thomas Beth, M. Frisch, and Gustavus J. Simmons, editors. *Public-key cryptography: state of the art and future directions: E.I.S.S workshop, Oberwolfach, Germany, July 3–6, 1991: final report*, volume 578 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. CODEN LNCSD9. ISBN 3-540-55215-4 (Berlin), 0-387-55215-4 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 P83 1992.

Beth:1992:PKC

[BFS92b] Thomas Beth, M. Frisch, and Gustavus J. Simmons, editors. *Public-key cryptography: state of the art and future directions: E.I.S.S workshop, Oberwolfach, Germany, July 3–6, 1991: final report*, volume 578 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. CODEN LNCSD9. ISBN 3-540-55215-4 (Berlin), 0-387-55215-4 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 P83 1992. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0578.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=578`.

Blundo:1996:TBC

[BFS96] C. Blundo, L. A. Frota Mattos, and D. R. Stinson. Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. *Lecture Notes in Computer Science*, 1109:387–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blundo:1998:GBC

[BFS98] C. Blundo, Luiz A. Frota Mattos, and D. R. Stinson. Generalized Beimel–Chor schemes for broadcast encryption and interactive key distribution. *Theoretical Computer Science*, 200(1–2):313–334, June 28, 1998. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cas/tree/store/tcs/sub/1998/200/1-2/2837.pdf`.

Busch:1999:DWC

[BFW99] Christoph Busch, Wolfgang Funk, and Stephen Wolthusen. Digital watermarking: From concepts to real-time video applications. *IEEE Computer Graphics and Applications*, 19(1):25–35, January/February 1999. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic). URL `http://computer.org/cga/cg1999/g1025abs.htm; http://dlib.computer.org/cg/`

books/cg1999/pdf/g1025.pdf.

Blum:1985:EPP

[BG85] Manuel Blum and Shafi Goldwasser. An efficient probabilistic public-key encryption scheme which hides all partial information. In Blakley and Chaum [BC85], pages 289–302. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=289. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Bellare:1990:NPD

[BG90] Mihir Bellare and Shafi Goldwasser. New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs. *Lecture Notes in Computer Science*, 435: 194–211, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350194.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350194.pdf.

Bellare:1993:DPK

[BG93] M. Bellare and O. Goldreich. On defining proofs of knowledge. *Lecture Notes in Computer Science*, 740: 390–420, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Baldwin:1998:PPR

[BG98] Robert W. Baldwin and James W. Gray, III. PCKS #14: Pseudo-random number generation. World-Wide Web slide presentation., October 1998. URL ftp://ftp.rsasecurity.com/pub/pkcs/98workshop/pkcs14_proposal3.ppt; ftp://ftp.rsasecurity.com/pub/pkcs/99workshop/workshop.zip.

Boyapati:1999:KSD

[BG99] V. Boyapati and R. Gore. KtSeqC: System description. *Lecture Notes in Computer Science*, 1617:29–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1994:ICC

[BGG94] Mihir Bellare, Oded Goldreich, and Shafi Goldwasser. Incremental cryptography: The case of hashing and signing. In Desmedt [Des94b], pages 216–233. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390216.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390216.pdf.

Bellare:1995:ICA

[BGG95] M. Bellare, O. Goldreich, and S. Goldwasser. Incremental cryptography and application to virus protection. In ACM [ACM95], pages 45–56. ISBN 0-89791-718-9. LCCN QA 76.6 A13 1995. ACM order no. 508950.

Bird:1991:SDT

[BGH+91] Ray Bird, Inder Gopal, Amir Herzberg, Phil Janson, Shay Kutten, Refik Molva, and Moti Yung. Systematic design of two-party authentication protocols. *Lecture Notes in Computer Science*, 576: 44–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760044.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760044.pdf.

Bird:1995:KFL

[BGH+95a] Ray Bird, Inder Gopal, Amir Herzberg, Phil Janson, Shay Kutten, Refik Molva, and Moti Yung. The KryptoKnight family of light-weight protocols for authentication and key distribution. *IEEE/ACM Transactions on Networking*, 3(1):31–41, February 1995. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL http://www.acm.org:80/pubs/citations/journals/ton/1995-3-1/p31-bird/.

Bruggermann:1995:VIS

[BGH95b] Hans H. Brüggermann and Waltraud Gerhardt-Häckl, editors. *Verlässliche IT-Systeme: proceedings der GI-Fachtagung VIS '95*. Vieweg & Son, Braunschweig, Germany, 1995. ISBN 3-528-05483-2. LCCN ????

Branstad:1977:RWC

[BGK77] Dennis K. Branstad, Jason Gait, and Stuart Katzke, editors. *Report of the*

Workshop on Cryptography in Support of Computer Security, held at the National Bureau of Standards, September 21–22, 1976. U.S. National Bureau of Standards, Gaithersburg, MD, USA, 1977.

Bellare:1999:SEP

[BGK99] M. Bellare, O. Goldreich, and H. Krawczyk. Stateless evaluation of pseudorandom functions: Security beyond the birthday barrier. In Wiener [Wie99], pages 270–287. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Bellare:1997:PNG

[BGM97a] M. Bellare, S. Goldwasser, and D. Micciancio. "pseudo-random" number generation within cryptographic algorithms: The DSS case. *Lecture Notes in Computer Science*, 1294:277–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1997:PRN

[BGM97b] Mihir Bellare, Shafi Goldwasser, and Daniele Micciancio. "pseudo-random" number generation within cryptographic algorithms: The DSS case. *Lecture Notes in Computer Science*, 1294:277–291, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940277.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940277.pdf`.

Bender:1996:TDH

[BGML96] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. *IBM Systems Journal*, 35(3–4):313–336, ???? 1996. CODEN IBMSA7. ISSN 0018-8670. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054106.html`.

Balkin:1994:CEC

[BGR94] Sandy D. Balkin, Elizabeth L. Golebiewski, and Clifford A. Reiter. Chaos and elliptic curves. *Computers and Graphics*, 18(1):113–117, January–February 1994. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic).

Bellare:1995:XMN

[BGR95] Mihir Bellare, Roch Guérin, and Phillip Rogaway. XOR MACs: New methods for message authentication using finite pseudorandom functions. In Coppersmith [Cop95d], pages 15–35. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-

3349 (electronic). LCCN QA76.9.A25 C79 1995. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=963. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Bellare:1998:BVA

[BGR98a] M. Bellare, J. A. Garay, and T. Rabin. Batch verification with applications to cryptography and checking. *Lecture Notes in Computer Science*, 1380:170–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1998:FBV

[BGR98b] Mihir Bellare, Juan A. Garay, and Tal Rabin. Fast batch verification for modular exponentiation and digital signatures. *Lecture Notes in Computer Science*, 1403:236–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030236.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030236.pdf.

Bierbrauer:1994:BRF

[BGS94] Jürgen Bierbrauer, K. Gopalakrishnan, and Douglas R. Stinson. Bounds for resilient functions and orthogonal arrays. In Desmedt [Des94b], pages 247–256. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390247.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390247.pdf.

Blundo:1995:DRR

[BGS95] C. Blundo, A. Giorgio Gaggia, and D. R. Stinson. On the dealer's randomness required in secret sharing schemes. *Lecture Notes in Computer Science*, 950: 35–46, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bierbrauer:1996:OAR

[BGS96] Jürgen Bierbrauer, K. Gopalakrishnan, and D. R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds. *SIAM Journal on Discrete Mathematics*, 9(3):424–452, August 1996. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Berkovits:1998:AMA

[BGS98] Shimshon Berkovits, Joshua D. Guttman, and Vipin Swarup. Authentication for mobile agents. *Lecture Notes in Computer Science*, 1419: 114–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1419/14190114.htm; http://link.springer-ny.com/link/service/series/0558/papers/1419/14190114.pdf`.

Benantar:1996:ACS

[BGT96] M. Benantar, R. Guski, and K. M. Troidle. Access control systems: From host-centric to network-centric computing. *IBM Systems Journal*, 35(1): 94–112, 1996. CODEN IBMSA7. ISSN 0018-8670. URL `http://www.research.ibm.com/journal/sj35-1.html#six`.

Bosselaers:1993:CWP

[BGV93] A. Bosselaers, R. Govaerts, and J. Vandewalle. Cryptography within phase I of the EEC-RACE programme. *Lecture Notes in Computer Science*, 741: 227–234, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bosselaers:1996:FHP

[BGV96] A. Bosselaers, R. Govaerts, and J. Vandewalle. Fast hashing on the Pentium. In Koblitz [Kob96], pages 298–312. CODEN LNCSD9. ISBN 3-540-61512-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1996. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1109.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1109`. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Biget:1997:HSC

[BGV97a] Patrick Biget, Patrick George, and Jean-Jacques Vandewalle. How smart cards can benefit from object-oriented technologies. *Future Generation Computer Systems*, 13(1): 75–90, June 1997. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.elsevier.com/gej-ng/10/19/19/28/17/21/abstract.html.

Bosselaers:1997:SDP

[BGV97b] A. Bosselaers, R. Govaerts, and J. Vandewalle. SHA: a design for parallel architectures? In Fumy [Fum97], pages 348–362. CODEN LNCSD9. ISBN 3-540-62975-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1997. Sponsored by the International Association for Cryptologic Research (IACR).

Beaver:1993:CPP

[BH93] Donald Beaver and Stuart Haber. Cryptographic protocols provably secure against dynamic adversaries. *Lecture Notes in Computer Science*, 658: 307–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580307.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580307.pdf.

Baker:1998:LTC

[BH98] Stewart Abercrombie Baker and Paul R. Hurst. *The limits of trust: cryptography, governments, and electronic commerce*. Kluwer Law International, Boston, 1998. ISBN 90-411-0635-9. xviii + 621 pp. LCCN K564.C6 B35 1998.

Beygelzimer:1999:OWF

[BHHR99] Alina Beygelzimer, Lane A. Hemaspaandra, Christopher M. Homan, and Jörg Rothe. One-way functions in worst-case cryptography: algebraic and security properties are on the house. *ACM SIGACT News*, 30 (4):25–40, December 1999. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Bhimani:1996:SCI

[Bhi96] Anish Bhimani. Securing the commercial Internet. *Communications of the Association for Computing Machinery*, 39(6): 29–35, June 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/228509.html; http://www.acm.org/pubs/toc/Abstracts/cacm/228509.html.

Boeleoni:1999:SBM

[BHJM99] L. Boeleoni, R. Hao, K. Jun,

and D. C. Marinescu. Structural biology metaphors applied to the design of a distributed object system. *Lecture Notes in Computer Science*, 1586:275–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Black:1999:UFS

[BHK+99] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway. UMAC: Fast and secure message authentication. In Wiener [Wie99], pages 216–233. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660216.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1666/16660216.pdf`.

Bubeck:1995:DSC

[BHKR95] T. Bubeck, M. Hiller, W. Kuchlin, and W. Rosenstiel. Distributed symbolic computation with DTS. In Ferreira and Rolim [FR95a], pages 231–248. ISBN 3-540-60321-2. LCCN QA76.642.I59 1995.

Bayer:1993:IER

[BHS93] D. Bayer, S. Haber, and W. S. Stornetta. Improving the efficiency and reliability of digital time-stamping. In R. M. Capocelli, A. De Santis, and U. Vaccaro, editors, *Sequences II: Methods in Communication, Security, and Computer Science*, pages 329–334. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993.

Bellare:1998:MTF

[BHSV98a] M. Bellare, S. Halevi, A. Sahai, and S. Vadhan. Many-to-one trapdoor functions and their relation to public-key cryptosystems. *Lecture Notes in Computer Science*, 1462:283–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1998:MOT

[BHSV98b] Mihir Bellare, Shai Halevi, Amit Sahai, and Salil Vadhan. Many-to-one trapdoor functions and their relation to public-key cryptosystems. *Lecture Notes in Computer Science*, 1462: 283–298, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620283.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1462/14620283.pdf`.

Brassard:1998:QCH

[BHT98] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. *Lecture Notes in Computer Science*, 1380: 163–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bertilsson:1993:CPS

[BI93] M. Bertilsson and I. Ingemarsson. A construction of practical secret sharing schemes using linear block codes. *Lecture Notes in Computer Science*, 718: 67–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bao:1994:RAF

[BI94] Feng Bao and Yoshihide Igarashi. A randomized algorithm to finite automata public key cryptosystem. *Lecture Notes in Computer Science*, 834:678–686, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bao:1995:BFA

[BI95] Feng Bao and Yoshihide Igarashi. Break finite automata public key cryptosystem. *Lecture Notes in Computer Science*, 944: 147–158, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Breitbach:1999:CCM

[BI99] Markus Breitbach and Hideki Imai. On channel capacity and modulation of watermarks in digital still images. *Lecture Notes in Computer Science*, 1648: 125–139, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1648/16480125.htm; http://link.springer-ny.com/link/service/series/0558/papers/1648/16480125.pdf`.

Bar-Ilan:1989:NFC

[BIB89] J. Bar-Ilan and D. Beaver. Non-cryptographic fault-tolerant computing in a constant number of rounds. In ACM [ACM89a], pages 201–209. ISBN 0-89791-326-4. LCCN QA 76.9 D5 A26 1989.

Biermann:1998:HKB

[Bie98] J. Biermann. Hades — a knowledge-based system for message interpretation and situation determination. *Lecture Notes in Computer Science*, 1416: 707–716, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1991:CCC

[Bih91] E. Biham. Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT '91. *Lecture Notes in Computer Science*, 547:532–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1992:DCI

[Bih92] Eli Biham. *Differential cryptanalysis of iterated cryptosystems*. Dissertation (Ph.D.), Department of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel, 1992. iii + 150 pp. URL `http://lib-phds1/Dissertations/biham_eli.pdf`.

Biham:1994:NTC

[Bih94a] E. Biham. New types of cryptanalytic attacks using related keys. *Lecture Notes in Computer Science*, 765:398–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1994:MOA

[Bih94b] Eli Biham. On modes of operation (abstract). In Anderson [And94a], pages 116–120. CODEN LNCSD9. ISBN 3-540-58108-1, 0-387-58108-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C36 1993.

Biham:1995:CMM

[Bih95a] E. Biham. Cryptanalysis of multiple modes of operation. *Lecture Notes in Computer Science*, 917: 278–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1995:MLC

[Bih95b] E. Biham. On Matsui's linear cryptanalysis. *Lecture Notes in Computer Science*, 950:341–355, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1996:CTM

[Bih96] Eli Biham. Cryptanalysis of triple modes of operation. Technical reports CS885, Technion, Haifa, Israil, August 1996. This is a preliminary version of [6].

Biham:1997:CL

[Bih97a] E. Biham. Cryptanalysis of Ladder-DES. *Lecture Notes in Computer Science*, 1267:134–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1997:FNI

[Bih97b] E. Biham. A fast new DES implementation in software. *Lecture Notes in Computer*

Science, 1267:260–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1997:FSE

[Bih97c] Eli Biham, editor. *Fast software encryption: 4th International Workshop, FSE '97, Haifa, Israel, January 20–22, 1997: proceedings*, volume 1267 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-63247-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25F77 1997.

Biham:1998:CMM

[Bih98a] Eli Biham. Cryptanalysis of multiple modes of operation. *Journal of Cryptology*, 11(1):45–58, Winter 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n1p45.html; http://link.springer.de/link/service/journals/00145/bibs/11n1p45.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n1p45.tex; http://link.springer.de/link/service/journals/00145/tocs/01101.html.

Biham:1998:IOS

[Bih98b] Eli Biham. Initial observation on Skipjack: cryptanalysis of Skipjack-3xor. Technical report 0946, Department of Computer Science, Technion-I.I.T., Haifa, Israel, 1998. 14 pp.

Biham:1999:CM

[Bih99a] Eli Biham. Cryptanalysis of MAGENTA. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Biham:1999:CTM

[Bih99b] Eli Biham. Cryptanalysis of triple modes of operation. *Journal of Cryptology*, 12(3):161–184, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n3p161.html; http://link.springer.de/link/service/journals/00145/papers/12n3p161.pdf.

Biham:1999:NCA

[Bih99c] Eli Biham. A note on comparing the AES candidates. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm`; `http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf`; `http://www.nist.gov/aes`. No slides for the conference talk are available.

Birrell:1985:SCU

[Bir85] Andrew D. Birrell. Secure communication using remote procedure calls. *ACM Transactions on Computer Systems*, 3(1):1–14, February 1985. CODEN ACSYEC. ISSN 0734-2071. URL `http://www.acm.org:80/pubs/citations/journals/tocs/1985-3-1/p1-birrell/`.

Biryukov:1995:CID

[Bir95] Alex Biryukov. Cryptanalysis and improvement of the Data Encryption Standard. Thesis (Master's), Faculty of mathematics, Technion — Israel Institute of Technology, Haifa, Israel, 1995. iii + 48 + 10 pp.

Birman:1998:ACH

[Bir98] Mark Birman. Accelerating cryptography in hardware: Public key, random number generation, symmetric key. In IEEE [IEE98b], page ?? ISBN ???? LCCN ????

Biryukov:1999:MC

[Bir99] Alex Biryukov. *Methods of cryptanalysis*. Thesis (Ph.D.), Faculty of Mathematics, Technion — Israel Institute of Technology, Haifa, Israel, 1999. 129 + 10 pp.

Bishop:1988:AFDa

[Bis88a] Matt Bishop. An application of a fast Data Encryption Standard implementation. Technical report PCS-TR 88-138, Department of Mathematics and Computer Science, Dartmouth College, Hanover, NH, USA, 1988. 25 pp.

Bishop:1988:AFDb

[Bis88b] Matt Bishop. An application of a fast data encryption standard implementation. In Association [Ass88], pages 221–254.

Bishop:1988:AFDc

[Bis88c] Matt Bishop. An application of a fast Data Encryption Standard implementation. *Computing Systems*, 1 (3):221–254, Summer 1988. CODEN CMSYE2. ISSN 0895-6340.

Bishop:COMPSYS-1-3-221

[Bis88d] Matt Bishop. An application of a fast data encryption standard implementation. *Computing Systems*, 1 (3):221–254, Summer 1988. CODEN CMSYE2. ISSN 0895-6340.

Bishop:1988:FEP

[Bis88e] Matt Bishop. The fast encryption package. Technical report, Research Institute for Advanced Computer Science, Moffett Field, CA, USA, 1988. various pp. RIACS memorandum 88.3, NASA contractor report NASA CR-185397.

Bishop:1989:USS

[Bis89a] M. Bishop. UNIX security in a supercomputing environment. In ACM [ACM89b], pages 693–698. ISBN 0-89791-341-8. LCCN QA 76.5 S87 1989. IEEE 89CH2802-7.

Bishop:1989:FEP

[Bis89b] Matt Bishop. *The fast encryption package*. Moffett Field, CA, USA, 1989. ?? pp. Microfiche.

Bishop:1990:AGD

[Bis90] Matt Bishop. Administrator's guide to the digital signature facility "rover". Technical report PCS-TR 90-153, Department of Mathematics and Computer Science, Dartmouth College, Hanover, NH, USA, 1990.

Bishop:1991:AMU

[Bis91] Matt Bishop. An authentication mechanism for USENET. In USENIX Association [USE91], pages 281–288. LCCN QA 76.76 O63 U84 1992.

Bishop:1992:FPC

[Bis92] Matt Bishop. Foiling Password Cracking. *UNIX/world*, 9(3):85–??, March 1992. ISSN 0739-5922.

Bleichenbache:1997:NOC

[BJQ97] D. Bleichenbache, M. Joye, and J.-J. Quisquater. A new and optimal chosen-message attack on RSA-type cryptosystems. *Lecture Notes in Computer Science*, 1334:302–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1997:ROZ

[BJY97] Mihir Bellare, Markus Jakobsson, and Moti Yung. Round-optimal zero-knowledge arguments based on any one-way function. *Lecture Notes in Computer Science*, 1233:280–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330280.htm; http://link.springer-ny.com/link/service/series/`

0558/papers/1233/12330280.pdf.

Book:1980:UDC

[BK80] R. V. Book and Sai Choi Kwan. On uniquely decipherable codes with two codewords. *IEEE Transactions on Computers*, C-29(4):324–325, April 1980. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1675571.

Bauspiess:1990:HKA

[BK90] Fritz Bauspieß and Hans-Joachim Knobloch. How to keep authenticity alive in a computer network. *Lecture Notes in Computer Science*, 434:38–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340038.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340038.pdf.

Blakley:1994:LAA

[BK94a] G. R. Blakley and G. A. Kabatianskii. Linear algebra approach to secret sharing schemes. *Lecture Notes in Computer Science*, 829:33–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brooks:1994:ST

[BK94b] Thomas A. Brooks and Michael M. Kaplan. Security technologies. *AT&T Technical Journal*, 73(5):4–8, September/October 1994. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Biham:1995:KPA

[BK95a] E. Biham and P. C. Kocher. A known plaintext attack on the PKZIP stream cipher. *Lecture Notes in Computer Science*, 1008:144–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blakley:1995:GPS

[BK95b] G. R. Blakley and G. A. Kabatianski. On general perfect secret sharing schemes. *Lecture Notes in Computer Science*, 963:367–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blum:1995:DPC

[BK95c] Manuel Blum and Sampath Kannan. Designing programs that check their work. *Journal of the Association for Computing Machinery*, 42(1):269–291, January 1995. CODEN JACOAH. ISSN 0004-

5411 (print), 1557-735X (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/200880.html.

Bocharova:1995:FEC

[BK95d] I. E. Bocharova and B. D. Kudryashov. Fast exponentiation in cryptography. *Lecture Notes in Computer Science*, 948:146–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Buydos:1997:C

[BK97] John F. Buydos and David Kahn. Cryptology. LC science tracer bullet TB 96-2, Science Reference Section, Science and Technology Division, Library of Congress, 101 Independence Ave., S.E., Washington, DC 20540-4750, USA, 1997. 15 pp. Caption title. Shipping list no.: 97-0345-P. "January 1997.".

Biham:1998:CAXa

[BK98a] Eli Biham and Lars R. Knudsen. Cryptanalysis of the ANSI X9.52 CBCM mode. Technical report 0928, Department of Computer Science — Israel Institute of Technology, Haifa, Israel, 1998. 11 pp.

Biham:1998:CAXb

[BK98b] Eli Biham and Lars R. Knudsen. Cryptanalysis of the ANSI X9.52 CBCM mode. In Nyberg [Nyb98], pages 100–?? ISBN 3-540-64518-7 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1403.

Biham:1998:TA

[BK98c] Eli Biham and Lars R. Knudsen. DES, triple-DES and AES. *CryptoBytes*, 4 (1):18–23, Summer 1998. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n1.pdf.

Biryukov:1998:DCC

[BK98d] A. Biryukov and E. Kushilevitz. From differential cryptanalysis to ciphertext-only attacks. *Lecture Notes in Computer Science*, 1462:72–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biryukov:1998:ICR

[BK98e] A. Biryukov and E. Kushilevitz. Improved cryptanalysis of RC5. *Lecture Notes in Computer Science*, 1403:85–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Buchholz:1998:TCF

[BK98f] Thomas Buchholz and Martin Kutrib. On time computability of functions in one-way cellular automata.

Acta Informatica, 35(4): 329–352, April 1998. CODEN AINFA2. ISSN 0001-5903 (print), 1432-0525 (electronic). URL http://link.springer-ny.com/link/service/journals/00236/bibs/8035004/80350329.htm; http://link.springer-ny.com/link/service/journals/00236/papers/8035004/80350329.pdf.

Buhler:1998:LBR

[BK98g] Joe Buhler and Neal Koblitz. Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems. *Bulletin of the Australian Mathematical Society*, 58(1):147–154, 1998. CODEN ALNBAB. ISSN 0004-9727.

Buchholz:1998:OGO

[BKK98] Thomas Buchholz, Andreas Klein, and Martin Kutrib. One guess one-way cellular arrays. *Lecture Notes in Computer Science*, 1450: 807–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1450/14500807.htm; http://link.springer-ny.com/link/service/series/0558/papers/1450/14500807.pdf.

Brown:1993:IRD

[BKPS93] Lawrence Brown, Matthew Kwan, Josef Pieprzyk, and Jennifer Seberry. Improving resistance to differential cryptanalysis and the redesign of LOKI. *Lecture Notes in Computer Science*, 739:36–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1994:SCB

[BKR94] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of cipher block chaining. In Desmedt [Des94b], pages 341–358. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390341.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390341.pdf.

Borst:1997:TAR

[BKR97] J. Borst, L. R. Knudsen, and V. Rijmen. Two attacks on reduced IDEA. *Lecture Notes in Computer Science*, 1233:1–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1998:LBI

[BKR98a] M. Bellare, T. Krovetz, and

P. Rogaway. Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible. *Lecture Notes in Computer Science*, 1403:266–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1998:LRB

[BKR98b] Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible. *Lecture Notes in Computer Science*, 1403: 266–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030266.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030266.pdf.

Bakhmurov:1999:DEE

[BKS99] A. Bakhmurov, A. Kapitonova, and R. Smeliansky. DYANA: An environment for embedded system design and analysis. *Lecture Notes in Computer Science*, 1579: 390–404, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Burgett:1998:CLD

[BKZ98] S. Burgett, E. Koch, and J. Zhao. Copyright labeling of digitized image data. *IEEE Communications Magazine*, 36(3):94–100, March 1998. CODEN ICOMD9. ISSN 0163-6804. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/071107.html.

Boneh:1995:QCH

[BL95] D. Boneh and R. J. Lipton. Quantum cryptanalysis of hidden linear functions. *Lecture Notes in Computer Science*, 963: 424–437, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://theory.stanford.edu/~dabo/papers/quantum.ps.gz.

Boneh:1996:ABF

[BL96a] D. Boneh and R. J. Lipton. Algorithms for black-box fields and their application to cryptography. *Lecture Notes in Computer Science*, 1109:283–297, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://theory.stanford.edu/~dabo/papers/bbf.ps.gz.

Boneh:1996:ABB

[BL96b] Dan Boneh and Richard J. Lipton. Algorithms for black-box fields and their application to cryptography. *Lecture Notes in Computer Science*, 1109: 283–297, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090283.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090283.pdf; http://theory.stanford.edu/~dabo/papers/bbf.ps.gz.

Binsted:1999:CDS

[BL99] Binsted and S. Luke. Character design for soccer commentary. *Lecture Notes in Computer Science*, 1604: 22–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blatman:1975:MMC

[Bla75] Peter Blatman. Method of modern cryptanalysis: research project. Thesis (M.S. in Electrical Engineering), Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA, June 1975. various pp.

Blakley:1979:SCK

[Bla79] G. R. Blakley. Safeguarding cryptographic keys. In Merwin et al. [MZS79], pages 313–317.

Blahut:1983:TPE

[Bla83] Richard E. Blahut. *Theory and Practice of Error Control Coding*. Addison-Wesley, Reading, MA, USA, 1983. ISBN 0-201-10102-5. xi + 500 pp. LCCN QA268 .B54 1983.

Blakley:1985:ITF

[Bla85] G. R. Blakley. Information theory without the finiteness assumption, I: Cryptosystems as group-theoretic objects. In Blakley and Chaum [BC85], pages 314–338. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=314. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Blanchard:1989:CSS

[Bla89] F. Blanchard. Certain sofic systems engendered codes. *Theoretical Computer Science*, 68(3):253–265, November 12, 1989. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Blaze:1993:TMS

[Bla93] Matt Blaze. Transparent mistrust: OS support for cryptography-in-the-large. In IEEE [IEE93a], pages 98–102. ISBN 0-8186-4000-6 (paper), 0-8186-4001-4 (microfiche). LCCN QA76.76.O63 W667 1993. URL `http://ieeexplore.ieee.org/iel2/918/8054/00348165.pdf`. IEEE catalog number 93TH0553-8.

Blackburn:1994:IRO

[Bla94a] Simon R. Blackburn. Increasing the rate of output of m-sequences. *Information Processing Letters*, 51 (2):73–77, July 26, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Blaze:1994:KME

[Bla94b] Matt Blaze. Key management in an encrypting file system. In USENIX [USE94], pages 27–35. ISBN 1-880446-62-6. LCCN QA 76.76 O63 U83 1994. URL `http://www.usenix.org/publications/library/proceedings/bos94/blaze.html`.

Blaze:1996:HBE

[Bla96a] M. Blaze. High-bandwidth encryption with low-bandwidth smartcards. *Lecture Notes in Computer Science*, 1039: 33–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blaze:1996:HEL

[Bla96b] M. Blaze. High-bandwidth encryption with low-bandwidth smartcards. *Lecture Notes in Computer Science*, 1039: 33–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blaze:1996:OKE

[Bla96c] M. Blaze. Oblivious key escrow. *Lecture Notes in Computer Science*, 1174: 335–343, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054407.html`.

Blair:1998:SEP

[Bla98] John Blair. Samba's encrypted password support. *Linux Journal*, 56:56–58, December 1998. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Bleichenbacher:1996:GES

[Ble96] D. Bleichenbacher. Generating ElGamal signatures without knowing the secret key. *Lecture Notes in Computer Science*, 1070:10–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bleichenbacher:1997:SKP

[Ble97] Daniel Bleichenbacher. On the security of the KMOV public key cryptosystem. *Lecture Notes in Computer Science*, 1294:235–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940235.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940235.pdf.

Bleichenbacher:1998:CCA

[Ble98a] Daniel Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. *Lecture Notes in Computer Science*, 1462:1–12, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620001.pdf.

Bleumer:1998:BYP

[Ble98b] Gerrit Bleumer. Biometric yet privacy protecting person authentication. *Lecture Notes in Computer Science*, 1525:99–110, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250099.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250099.pdf.

Barber:1999:AOD

[BLH99] K. S. Barber, T. H. Liu, and D. C. Han. Agent-oriented design. *Lecture Notes in Computer Science*, 1647:28–40, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Buldas:1998:TBL

[BLLV98] A. Buldas, P. Laud, H. Lipmaa, and J. Villemson. Time-stamping with binary linking schemes. *Lecture Notes in Computer Science*, 1462:486–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beth:1994:CCB

[BLM94] Thomas Beth, D. E. Lazic, and A. Mathias. Cryptanalysis of cryptosystems based on remote chaos replication. In Desmedt [Des94b], pages 318–331. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390318.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0839/08390318.pdf`.

Baaz:1999:SDC

[BLM99] M. Baaz, A. Leitsch, and G. Moser. System description: CutRes 0.1: Cut elimination by resolution. *Lecture Notes in Computer Science*, 1632:212–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brassil:1994:EMI

[BLMO94] J. Brassil, S. Low, N. Maxemchuk, and L. O'Garman. Electronic marking and identification techniques to discourage document copying. In IEEE [IEE94f], pages 1278–1287. ISBN 0-8186-5571-2 (microfiche). LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/034110.html`. Three volumes. IEEE Computer Society Press Order Number 5570-02. IEEE Catalog Number 94CH3401-7.

Brassil:1995:HID

[BLMO95] J. Brassil, S. Low, N. F. Maxemchuk, and L. O'Gorman. Hiding information in document images. In Anonymous [Ano95r], pages 482–489. LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1040.html`.

Brickell:1983:EAA

[BLO83] E. F. Brickell, J. C. Lagarias, and A. M. Odlyzko. Evaluation of the Adleman attack on multiply iterated knapsack cryptosystems. In Chaum et al. [CRS83], pages 39–42. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982.

Brickell:1984:EAA

[BLO84] E. F. Brickell, J. C. Lagarias, and A. M. Odlyzko. Evaluation of the Adleman attack on multiply iterated knapsack cryptosystems (abstract). In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 39–42. Plenum, New York, 1984.

Bloch:1998:EAU

[Blo98a] Gilbert Bloch. Enigma avant ULTRA: (Enigma before ULTRA). In Deavours et al. [DKK+98], pages 395–401. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Bloch:1998:EBUa

[Blo98b] Gilbert Bloch. Enigma before ULTRA: Polish work and the French contribution. In Deavours et al. [DKK+98], pages 373–386. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Bloch:1998:EBUb

[Blo98c] Gilbert Bloch. Enigma before ULTRA: the Polish success and check (1933–1939). In Deavours et al. [DKK+98], pages 387–394. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Bloch:1999:FMF

[Blo99] I. Bloch. Fuzzy morphology and fuzzy distances: New definitions and links in both Euclidean and geodesic cases. *Lecture Notes in Computer Science*, 1566:149–165, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brillhart:1975:NPC

[BLS75] John Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Mathematics of Computation*, 29(130):620–647, April 1975. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Blum:1982:CFT

[Blu82] Manuel Blum. Coin flipping by telephone — a protocol for solving impossible problems. In Rudolph [Rud82], pages 133–137. ISBN ???? LCCN TK7885.A1 C53 1982. IEEE catalog number 82CH1739-2.

Blum:1983:CFT

[Blu83a] Manuel Blum. Coin flipping by telephone — a protocol for solving impossible problems. *ACM SIGACT News*, 15(1):23–27, January 1983. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Blum:1983:HES

[Blu83b] Manuel Blum. How to exchange (secret) keys. *ACM Transactions on Computer Systems*, 1(2):175–193, May 1983. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic). Previously published in ACM STOC '83 proceedings, pages 440–447.

Blum:1984:IUC

[Blu84] Manuel Blum. Independent unbiased coin flips from a correlated biased source: a finite state Markov chain. In IEEE [IEE84], pages 425–433. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.

Blundo:1995:NDT

[Blu95] Carlo Blundo. A note on dynamic threshold schemes. *Information Processing Letters*, 55(4):189–193, August 25, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Blundon:1997:BCE

[Blu97] William Blundon. Blundon's corner: eciphering the NC world. *JavaWorld: IDG's magazine for the Java community*, 2(3): ??, March 1997. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/jw-03-1997/jw-03-blundon.htm`.

Bayer:1975:EST

[BM75] Rudolf Bayer and J. K. Metzger. On the encipherment of search trees and random access files. In Kerr [Ker75], page 452. ISBN ???? ISSN 0278-2596. LCCN QA76.9.D3 I55 1975. US$15.00. URL `http://www.vldb.org/dblp/db/conf/vldb/BayerM75.html`.

Bayer:1976:EST

[BM76] R. Bayer and J. K. Metzger. On the encipherment of search trees and random access files. *ACM Transactions on Database Systems*, 1(1):37–52, March 1976. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1976-1-1/p37-bayer/p37-bayer.pdf; http://www.acm.org/pubs/citations/journals/tods/1976-1-1/p37-bayer/`. Also published in [Ker75, p. 508–510].

Blum:1982:HGC

[BM82] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. In IEEE [IEE82a], pages 112–117. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

Blum:1984:HGC

[BM84a] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4):850–864, ???? 1984. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Boyer:1984:PCR

[BM84b] Robert S. Boyer and J. Strother Moore. Proof checking the RSA public key encryption algorithm. *American Mathematical Monthly*, 91(3):181–189, 1984. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Blakley:1985:SRS

[BM85] G. R. Blakley and Catherine Meadows. Security of ramp schemes. In Blakley and Chaum [BC85], pages 242–268. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=242. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Beale:1989:EUR

[BM89] M. Beale and M. F. Monaghan. Encryption using random Boolean functions. In *Cryptography and coding (Cirencester, 1986)*, volume 20 of *Inst. Math. Appl. Conf. Ser. New Ser.*, pages 219–230. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1989.

Bellare:1990:NIO

[BM90] Mihir Bellare and Silvio Micali. Non-interactive oblivious transfer and applications. *Lecture Notes in Computer Science*, 435: 547–557, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350194.htm; http://link.springer-ny.com/link/service/series/

0558/papers/0435/04350194.pdf.

Bellovin:1991:LKA

[BM91a] Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. In USENIX Association [USE91], pages 253–267. LCCN QA 76.76 O63 U84 1992. URL ftp://research.bell-labs.com/dist/kerblimit.usenix.ps.Z; local --- kerblimit.usenix.ps. FTP - research.att.com:/dist/kerblimit.usenix.ps.Z; local - kerblimit.usenix.ps.

Brickell:1991:IID

[BM91b] E. F. Brickell and K. S. McCurley. Interactive identification and digital signatures. *AT&T Technical Journal*, 70(6):73–86, November/December 1991. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Bellare:1992:HSG

[BM92] Mihir Bellare and Silvio Micali. How to sign given any trapdoor permutation. *Journal of the Association for Computing Machinery*, 39(1):214–233, January 1992. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/147537.html.

Bleichenbacher:1994:DAG

[BM94a] Daniel Bleichenbacher and Ueli M. Maurer. Directed acyclic graphs, one-way functions and digital signatures. In Desmedt [Des94b], pages 75–82. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390075.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390075.pdf.

Boyd:1994:DSK

[BM94b] C. Boyd and W. Mao. Designing secure key exchange protocols. *Lecture Notes in Computer Science*, 875:93–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Burns:1994:PSS

[BM94c] J. Burns and C. J. Mitchell. Parameter selection for server-aided RSA computation schemes. *IEEE Transactions on Computers*, 43(2):163–174, February 1994. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.

org/stamp/stamp.jsp?tp=&arnumber=262121.

Boyd:1995:DAK

[BM95] C. Boyd and W. Mao. Design and analysis of key exchange protocols via secure channel identification. *Lecture Notes in Computer Science*, 917:171–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bleichenbacher:1996:EOT

[BM96a] D. Bleichenbacher and U. Maurer. On the efficiency of one-time digital signatures. *Lecture Notes in Computer Science*, 1163:145–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bleichenbacher:1996:OTB

[BM96b] D. Bleichenbacher and U. M. Maurer. Optimal tree-based one-time digital signature schemes. *Lecture Notes in Computer Science*, 1046:363–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bleichenbacher:1996:OTO

[BM96c] D. Bleichenbacher and U. M. Maurer. Optimal tree-based one-time digital signature schemes. *Lecture Notes in Computer Science*, 1046:363–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brincat:1997:SC

[BM97] K. Brincat and A. Meijer. On the SAFER cryptosystem. *Lecture Notes in Computer Science*, 1355:59–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1999:FDS

[BM99a] M. Bellare and S. K. Miner. A forward-secure digital signature scheme. In Wiener [Wie99], pages 431–448. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Bellare:1999:FSD

[BM99b] Mihir Bellare and Sara K. Miner. A forward-secure digital signature scheme. *Lecture Notes in Computer Science*, 1666:431–448, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660431.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660431.pdf.

Blundo:1999:RMS

[BM99c] C. Blundo and B. Masucci. Randomness in multi-secret sharing schemes. *J.UCS:*

Journal of Universal Computer Science, 5(7):367–389, July 28, 1999. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL `http://www.jucs.org/jucs_5_7/randomness_in_multi_secret`.

Blackburn:19xx:NPP

[BMxx] Simon R. Blackburn and Sean Murphy. The number of partitions in Pollard rho. Private communication., 19xx.

Bento:1995:RCI

[BMC95] C. Bento, L. Macedo, and E. Costa. Reasoning with cases imperfectly described and explained. *Lecture Notes in Computer Science*, 984:45–59, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beimel:1999:ANN

[BMM99a] A. Beimel, T. Malkin, and S. Micali. The all-or-nothing nature of two-party secure computation. *Lecture Notes in Computer Science*, 1666:80–97, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beimel:1999:ANT

[BMM99b] A. Beimel, T. Malkin, and S. Micali. The all-or-nothing nature of two-party secure computation. In Wiener [Wie99], pages 80–97. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Bhowmick:1999:WWD

[BMNL99] S. S. Bhowmick, S. K. Madria, W.-K. Ng, and E.-P. Lim. Web warehousing: Design and issues. *Lecture Notes in Computer Science*, 1552:93–104, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blackburn:1997:CNP

[BMP97a] S. R. Blackburn, S. Murphy, and K. G. Paterson. A comment on "A new public-key cipher system based upon the Diophantine equations". *IEEE Transactions on Computers*, 46(4):512, April 1997. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=588077`. See [LCL95].

Blackburn:1997:CTA

[BMP+97b] S. R. Blackburn, S. Murphy, K. G. Paterson, S. Nandi, and P. P. Chaudhuri. Comments on "Theory and applications of cellular automata in cryptography" [and reply]. *IEEE Transactions on Computers*, 46

(5):637–639, May 1997. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=589245. See [NKC94, NC97].

Biedl:1998:GMF

[BMRW98] T. Biedl, J. Marks, K. Ryall, and S. Whitesides. Graph multidrawing: Finding nice drawings without defining nice. *Lecture Notes in Computer Science*, 1547: 347–355, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blackburn:1994:WPK

[BMS94] Simon Blackburn, Sean Murphy, and Jacques Stern. Weaknesses of a public-key cryptosystem based on factorizations of finite groups. *Lecture Notes in Computer Science*, 765: 50–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650050.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650050.pdf.

Blundo:1996:TOB

[BMS96] Carlo Blundo, Luiz A. Frota Mattos, and Douglas R. Stinson. Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. In *Advances in cryptology—CRYPTO '96 (Santa Barbara, CA)*, volume 1109 of *Lecture Notes in Comput. Sci.*, pages 387–400. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090387.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090387.pdf.

Bubak:1999:DHP

[BMS99] M. Bubak, J. T. Moscicki, and J. Shiers. Design of high-performance C++ package for handling of multidimensional histograms. *Lecture Notes in Computer Science*, 1593:543–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biehl:1996:CPB

[BMT96] I. Biehl, B. Meyer, and C. Thiel. Cryptographic protocols based on real-quadratic *A*-fields. *Lecture Notes in Computer Science*, 1163:15–??, 1996. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Barker:1998:TKL

[BMT98] R. Barker, A. Meehan, and I. Tranter. Towards a knowledge-level model for concurrent design. *Lecture Notes in Computer Science*, 1415:57–67, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blake:1985:CLG

[BMV85] I. F. Blake, R. C. Mullin, and S. A. Vanstone. Computing logarithms in GF(2^n). In Blakley and Chaum [BC85], pages 73–82. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=73`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Boppana:1996:BCP

[BN96] Ravi B. Boppana and Babu O. Narayanan. The biased coin problem. *SIAM Journal on Discrete Mathematics*, 9(1):29–36, February 1996. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Busch:1999:GEI

[BNP99] Christoph Busch, Klara Nahrstedt, and Ioannis Pitas. Guest Editors' introduction: Image security. *IEEE Computer Graphics and Applications*, 19(1):16–17, January/February 1999. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic). URL `http://dlib.computer.org/cg/books/cg1999/pdf/g1016.pdf`.

Book:1985:SNP

[BO85a] R. V. Book and F. Otto. On the security of name-stamp protocols. *Theoretical Computer Science*, 39(2-3):319–325, August 1985. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Book:1985:SNS

[BO85b] R. V. Book and F. Otto. On the security of name-stamp protocols. *Theoretical Computer Science*, 39(2-3):319–325, August 1985. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Book:1985:VTA

[BO85c] R. V. Book and F. Otto. On the verifiability of two-party algebraic protocols. *Theoretical Computer Science*, 40(2-3):101–130, ???? 1985. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Book:1985:CRE

[BO85d] Ronald V. Book and Friedrich Otto. Cancellation rules and extended word problems. *Information Processing Letters*, 20 (1):5–11, January 2, 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Brickell:1988:CSR

[BO88] Ernest F. Brickell and Andrew M. Odlyzko. Cryptanalysis: a survey of recent results. *Proceedings of the IEEE*, 76(5):578–593, May 1988. CODEN IEEPAD. ISSN 0018-9219 (print), 1558-2256 (electronic).

Brickell:1992:CSR

[BO92] E. F. Brickell and A. M. Odlyzko. Cryptanalysis: a survey of recent results. In Simmons [Sim92], pages 501–540. ISBN 0-87942-277-7. LCCN QA76.9.A25 C6678 1992. US$79.95. URL `http://www.research.att.com/~amo/doc/arch/cryptanalysis.surv.pdf`; `http://www.research.att.com/~amo/doc/arch/cryptanalysis.surv.ps`; `http://www.research.att.com/~amo/doc/arch/cryptanalysis.surv.tex`. IEEE order number: PC0271-7.

Berghel:1996:IKP

[BO96a] H. Berghel and L. O'Gorman. Internet kiosk: Protecting ownership rights through digital watermarking. *Computer*, 29(7):101–103, July 1996. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/053105.html`.

Brassil:1996:WDI

[BO96b] J. Brassil and L. O'Gorman. Watermarking document images with bounding box expansion. In Anderson [And96c], pages 227–235. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054111.html`.

Bull:1999:NMA

[BO99] John A. Bull and David J. Otway. A nested mutual authentication protocol. *Operating Systems*

Review, 33(4):42–47, October 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Ben-Or:1983:CSS

[BOCS83] Michael Ben-Or, Benny Chor, and Adi Shamir. On the cryptographic security of single RSA bits. In ACM [ACM83], pages 421–430. ISBN 0-89791-099-0. LCCN QA75.5.A14 1983. ACM order no. 508830.

Boland:1995:WDI

[BOD95] F. M. Boland, J. J. K. O.Ruanaidh, and C. Dautzenberg. Watermarking digital images for copyright protection. In IEE [IEE95a], pages 326–330. CODEN IECPB4. ISBN 0-85296-642-3. ISSN 0537-9989. LCCN ????

Ben-Or:1990:EPP

[BOGG+90] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali, and P. Rogaway. Everything provable is provable in zero-knowledge. In Goldwasser [Gol90b], pages 37–56. CODEN LNCSD9. ISBN 0-387-97196-3 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1988. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0403.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=403`.

Ben-Or:1988:MIP

[BOGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove intractability. In ACM [ACM88], pages 113–131. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order no. 508880.

Ben-Or:1988:CTN

[BOGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computations. In ACM [ACM88], pages 1–10. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order no. 508880.

Bolignano:1997:TMC

[Bol97] D. Bolignano. Towards a mechanization of cryptographic protocol verification. *Lecture Notes in Computer Science*, 1254:131–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bolignano:1998:IPB

[Bol98a] D. Bolignano. Integrating proof-based and model-checking techniques for the formal verification of cryptographic protocols. *Lecture Notes in Computer Science*, 1427:77–??, 1998. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Bolignano:1998:IPM

[Bol98b] D. Bolignano. Integrating proof-based and model-checking techniques for the formal verification of cryptographic protocols. *Lecture Notes in Computer Science*, 1427:77–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bond:1947:FSC

[Bon47] Raymond T. (Raymond Tostevin) Bond. *Famous stories of code and cipher*. Rinehart and Company, New York; Toronto, 1947. xxvi + 342 pp. LCCN PS648.C6 B65. Reprinted in 1965 by Collier Books.

Boneh:1998:DDP

[Bon98a] D. Boneh. The decision Diffie–Hellman problem. *Lecture Notes in Computer Science*, 1423: 48–63, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://theory.stanford.edu/~dabo/papers/DDH.ps.gz`.

Boneh:1998:DDH

[Bon98b] Dan Boneh. The decision Diffie–Hellman problem. *Lecture Notes in Computer Science*, 1423: 48–63, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1423/14230048.htm; http://link.springer-ny.com/link/service/series/0558/papers/1423/14230048.pdf; http://theory.stanford.edu/~dabo/papers/DDH.ps.gz`.

Boneh:1999:TYA

[Bon99] Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the American Mathematical Society*, 46(2):203–213, February 1999. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL `http://theory.stanford.edu/~dabo/papers/RSA-survey.pdf; http://theory.stanford.edu/~dabo/papers/RSA-survey.ps`.

Booth:1981:ASU

[Boo81] K. S. Booth. Authentication of signatures using public key encryption. *Communications of the Association for Computing Machinery*, 24(11):772–774, November 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bookstein:1996:RB

[Boo96] A. Bookstein. Research: Bibliocryptography. *Journal of the American Society for Information Science*, 47(12):886–895, December 1996. CODEN AISJB6. ISSN 0002-8231 (print), 1097-4571 (electronic).

Borman:1993:RTAa

[Bor93a] D. Borman. RFC 1409: Telnet Authentication Option, January 1993. URL ftp://ftp.internic.net/rfc/rfc1409.txt; ftp://ftp.internic.net/rfc/rfc1416.txt; https://www.math.utah.edu/pub/rfc/rfc1409.txt; https://www.math.utah.edu/pub/rfc/rfc1416.txt. Obsoleted by RFC1416 [Bor93c]. Status: EXPERIMENTAL.

Borman:1993:RTAb

[Bor93b] D. Borman. RFC 1411: Telnet Authentication: Kerberos Version 4, January 1993. URL ftp://ftp.internic.net/rfc/rfc1411.txt; https://www.math.utah.edu/pub/rfc/rfc1411.txt. Status: EXPERIMENTAL.

Borman:1993:RTAc

[Bor93c] D. Borman. RFC 1416: Telnet Authentication Option, February 1993. URL ftp://ftp.internic.net/rfc/rfc1409.txt; ftp://ftp.internic.net/rfc/rfc1416.txt; https://www.math.utah.edu/pub/rfc/rfc1409.txt; https://www.math.utah.edu/pub/rfc/rfc1416.txt. Obsoletes RFC1409 [Bor93a]. Status: EXPERIMENTAL.

Borcherding:1995:NAR

[Bor95] M. Borcherding. On the number of authenticated rounds in Byzantine agreement. *Lecture Notes in Computer Science*, 972: 230–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Borcherding:1996:LAD

[Bor96] M. Borcherding. Levels of authentication in distributed agreement. *Lecture Notes in Computer Science*, 1151:40–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bosworth:1982:CCC

[Bos82] Bruce Bosworth. *Codes, ciphers, and computers: an introduction to information security*. Hayden Book Co., Rochelle Park, NJ, USA, 1982. ISBN 0-8104-5149-2. 259 pp. LCCN Z103.B58 1982.

Bosma:1990:PPC

[Bos90] W. Bosma. *Primality Proving with Cyclotomy*. Doctoral dissertation, University of Amsterdam, Amsterdam, The Netherlands, 1990. ?? pp.

Bosselaers:19xx:EFH

[Bosxx] A. Bosselaers. Even faster hashing on the Pentium. In *????*, page ?? ????, ????, 19xx. ISBN ???? LCCN ???? URL `ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/bosselae/pentiumplus.ps.gz`. Presented at the rump session of Eurocrypt'97, Konstanz, Germany, May 12-15, 1997, and updated on November 13, 1997.

Bounas:1985:DDS

[Bou85] Adam C. Bounas. Direct determination of a "seed" binary matrix. *Information Processing Letters*, 20 (1):47–50, January 2, 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Boucher:1994:GPA

[Bou94] M. Boucher. La génération pseudo-aléatoire cryptographiquement sécuritaire et ses considérations pratiques. (French) [Cryptographically-secure random-number generation and its practical considerations]. Masters thesis, Département d'I.R.O., Université de Montréal, Montréal, QC, Canada, 1994.

Bovelander:1998:SCS

[Bov98a] Ernst Bovelander. Smart card security. *Lecture Notes in Computer Science*, 1528: 332–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1528/15280332.htm; http://link.springer-ny.com/link/service/series/0558/papers/1528/15280332.pdf`.

Bovenlander:1998:SCS

[Bov98b] E. Bovenlander. Smart card security. *Lecture Notes in Computer Science*, 1528: 332–337, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bowers:1959:DSP

[Bow59] William Maxwell Bowers. *Digraphic substitution: the Playfair cipher, the four square cipher*. Practical cryptanalysis; v. 1. American Cryptogram Association, Greenfield, MA, USA, 1959. 46 pp.

Bowers:1960:BC

[Bow60a] William Maxwell Bowers. *The bifid cipher*. Practical cryptanalysis; v. 2. American Cryptogram Association, Greenfield, MA, USA, 1960. 48 pp.

Bowers:1960:TC

[Bow60b] William Maxwell Bowers. *The trifid cipher*. Practical cryptanalysis; v. 3. American Cryptogram Association, Greenfield, MA, USA, 1960. ix + 55 pp.

Bowling:1993:SEA

[Bow93] Brian D. Bowling. The secure encryption algorithm. Thesis (M.S.), University of Cincinnati, Cincinnati, OH, USA, 1993. 63 pp.

Bowers:19xx:PC

[Bowxx] William Maxwell Bowers. *Practical cryptanalysis*. ????, Clarksburg, WV, USA, 19xx. 21 + 18 + 61 + 57 pp.

Boyd:1986:CPC

[Boy86] Waldo T. Boyd. *Cryptology and the personal computer: with programming in Basic*, volume 47 of *A Cryptographic Series*. Aegean Park Press, Laguna Hills, CA, USA, 1986. ISBN 0-89412-145-6 (hardcover), 0-89412-144-8 (paperback). 157 pp. LCCN ????

Boyd:1988:CCB

[Boy88] Waldo T. Boyd. *Computer cryptology: beyond decoder rings*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1988. ISBN 0-13-166133-7 (paperback). xv + 268 pp. LCCN Z103 .B65 1988. US$21.95.

Boyar:1989:ISPb

[Boy89a] Joan Boyar. Inferring sequences produced by a linear congruential generator missing low-order bits. *Journal of Cryptology*, 1 (3):177–184, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Boyar:1989:ISPa

[Boy89b] Joan Boyar. Inferring sequences produced by pseudo-random number generators. *Journal of the Association for Computing Machinery*, 36(1):129–141, January 1989. CODEN JACOAH. ISSN 0004-5411. URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/59305.html; http://www.imada.sdu.dk/~joan/`.

Boyd:1990:NMK

[Boy90] Colin Boyd. A new multiple key cipher and an improved voting scheme. *Lecture Notes in Computer Science*, 434:617–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340617.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340617.pdf`.

Boyd:1992:FFA

[Boy92] Colin Boyd. A formal framework for authentication. *Lecture Notes in Computer Science*, 648:273–??, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boyd:1995:CCC

[Boy95a] C. Boyd, editor. *Cryptography and coding: 5th Conference — December 1995, Cirencester*, number 1025 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-60693-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C76 1995.

Boyd:1995:CCI

[Boy95b] Colin Boyd, editor. *Cryptography and coding: 5th IMA conference, Cirencester, UK, December 18–20, 1995, proceedings*, volume 1025 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-60693-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C76 1995. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1025.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1025`. Papers from the 5th IMA Conference on Cryptography and Coding.

Boyd:1997:DSP

[Boy97] C. Boyd. Digital signature and public key cryptosystem in a prime order subgroup of Zn0*. *Lecture Notes in Computer Science*, 1334:346–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boyer:1998:DSM

[Boy98] John Boyer. Digital signatures with the Microsoft CryptoAPI: Adding security to Windows applications. *Dr. Dobb's Journal of Software Tools*, 23(6):80, 82–85, June 1998. CODEN DDJOEB. ISSN 1044-789X.

Boyko:1999:SPO

[Boy99] V. Boyko. On the security properties of OAEP as an all-or-nothing transform. In Wiener [Wie99], pages 503–518. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Beker:1982:CSP

[BP82] Henry Beker and F. C. (Frederick Charles) Piper. *Cipher systems: the protection of communications.*

John Wiley and Sons, Inc., New York, NY, USA, 1982. ISBN 0-471-89192-4. 427 pp. LCCN Z104 .B39 1982.

Beker:1985:SSC

[BP85] Henry Beker and F. C. (Frederick Charles) Piper. *Secure speech communications*, volume 3 of *Microelectronics and signal processing*. Academic Press, New York, NY, USA, 1985. ISBN 0-12-084780-9. xi + 267 pp. LCCN TK5102.5 .B354 1985.

Beker:1989:CC

[BP89] Henry Beker and F. C. Piper, editors. *Cryptography and coding*, The Institute of Mathematics and Its Applications conference series; new ser., 20. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1989. ISBN 0-19-853623-2. LCCN QA268.C74 1989. UK£35.00, US$52.00. Held in December 1986. "Based on the proceedings of a conference organized by the Institute of Mathematics and its Applications on cryptography and coding, held at the Royal Agricultural College, Cirencester on 15th-17th December 1986.".

Bilchev:1995:ACM

[BP95a] G. Bilchev and I. C. Parmee. The ant colony metaphor for searching continuous design spaces. *Lecture Notes in Computer Science*, 993:25–39, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bosselaers:1995:IPS

[BP95b] Antoon Bosselaers and Bart Preneel, editors. *Integrity primitives for secure information systems: final RIPE report of RACE Integrity Primitives Evaluation (R1040)*, volume 1007 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-60640-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). 239 pp. LCCN QA76.9.A25 I553 1995.

Baric:1997:CAF

[BP97a] N. Baric and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. *Lecture Notes in Computer Science*, 1233: 480–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brinkley:1997:SFS

[BP97b] James F. Brinkley and Jeffrey S. Prothero. Slisp: a flexible software toolkit for hybrid, embedded and distributed applications. *Software—Practice and Experience*, 27(1):33–48, January 1997. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Buchmann:1997:OWF

[BP97c] J. Buchmann and S. Paulus. A one way function based on ideal arithmetic in number fields. *Lecture Notes in Computer Science*, 1294: 385–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bailey:1998:OEF

[BP98a] Daniel V. Bailey and Christof Paar. Optimal extension fields for fast arithmetic in public-key algorithms. *Lecture Notes in Computer Science*, 1462: 472–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620472.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620472.pdf`.

Barnett:1998:AOD

[BP98b] R. Barnett and D. Pearson. Attack operators for digitally watermarked images. *IEE proceedings. Vision, image, and signal processing*, 145(4):271–279, August 1998. CODEN IVIPEK. ISSN 1350-245X.

Barnett:1998:FML

[BP98c] R. Barnett and D. E. Pearson. Frequency mode LR attack operator for digitally watermarked images. *Electronics Letters*, 34(19):1837–1839, September 1998. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic).

Bassia:1998:RAW

[BP98d] P. Bassia and I. Pitas. Robust audio watermarking in the time domain. In Theodoridis et al. [T+98], pages 25–28. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073110.html`. Four volumes.

Bella:1998:KVI

[BP98e] G. Bella and L. C. Paulson. Kerberos Version IV: Inductive analysis of the secrecy goals. *Lecture Notes in Computer Science*, 1485: 361–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bella:1998:MBK

[BP98f] G. Bella and L. C. Paulson. Mechanising BAN Kerberos by the inductive method. *Lecture Notes in Computer Science*, 1427:416–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bleichenbacher:1999:SC

[BP99a] D. Bleichenbacher and S. Patel. SOBER cryptanalysis. In Knudsen [Knu99c], pages 305–316. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Blum:1999:MME

[BP99b] T. Blum and C. Paar. Montgomery modular exponentiation on reconfigurable hardware. In Koren and Kornerup [KK99b], pages 70–77. ISBN 0-7803-5609-8, 0-7695-0116-8, 0-7695-0118-4. ISSN 1063-6889. LCCN QA76.6 .S887 1999. URL `http://euler.ecs.umass.edu/paper/final/paper-133.pdf; http://euler.ecs.umass.edu/paper/final/paper-133.ps`. IEEE Computer Society Order Number PR00116. IEEE Order Plan Catalog Number 99CB36336.

Birov:1999:PML

[BPBV99] L. Birov, A. Prokofiev, Y. Bartenev, and A. Vargin. The parallel mathematical libraries project (PMLP): Overview, design innovations, and preliminary results. *Lecture Notes in Computer Science*, 1662: 186–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blaze:1999:KNT

[BPK99] M. Blaze, J. Pigenbaum, and A. D. Keromytis. Key note: Trust management for public-key infrastructures. *Lecture Notes in Computer Science*, 1550:59–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bishr:1999:PRS

[BPR99] Y. A. Bishr, H. Pundt, and C. Ruether. Proceeding on the road of semantic interoperability — design of a semantic mapper based on a case study from transportation. *Lecture Notes in Computer Science*, 1580: 203–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blobel:1999:SAD

[BPRF99] B. Blobel, P. Pharow, and F. Roger-France. Security analysis and design based on a general conceptual security model and UML. *Lecture Notes in Computer Science*, 1593:919–??, 1999. CODEN LNCSD9. ISSN

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

Brown:1998:LA

[BPS98] Lawrie Brown, Josef Pieprzyk, and Jennifer Seberry. LOKI97 — AES1. In National Institute of Standards and Technology [Nat98], page 21. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf1/loki97-slides.pdf. Only the slides for the conference talk are available.

Borst:1999:LCR

[BPV99] J. Borst, B. Preneel, and J. Vandewalle. Linear cryptanalysis of RC5 and RC6. In Knudsen [Knu99c], pages 16–30. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Beguin:1995:FSR

[BQ95a] P. Beguin and J.-J. Quisquater. Fast server-aided RSA signatures secure against active attacks. *Lecture Notes in Computer Science*, 963: 57–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beguin:1995:FSA

[BQ95b] Philippe Béguin and Jean-Jacques Quisquater. Fast server-aided RSA signatures secure against active attacks. *Lecture Notes in Computer Science*, 963: 57–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630057.htm; http://link.springer-ny.com/link/service/series/0558/papers/0963/09630057.pdf.

Blakley:1988:CBA

[BR88] G. R. Blakley and William Rundell. Cryptosystems based on an analog of heat flow. *Lecture Notes in Computer Science*, 293: 306–329, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beutelspacher:1991:EFS

[BR91] Albrecht Beutelspacher and Ute Rosenbaum. Essentially ℓ-fold secure authentication systems. *Lecture Notes in Computer Science*, 473:294–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730294.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730294.pdf.

Bellare:1994:EAK

[BR94a] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In Desmedt [Des94b], pages 232–249. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730232.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730232.pdf.

Bellare:1994:OAEa

[BR94b] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. Research report RC 19610 (86198), IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, June 16, 1994. 19 pp. Appears in Advances in Cryptology — Eurocrypt 94 Proceedings, 1994.

Bellare:1995:OAE

[BR95a] M. Bellare and P. Rogaway. Optimal asymmetric encryption: How to encrypt with RSA. In De Santis [De 95], pages 92–111. CODEN LNCSD9. ISBN 3-540-60176-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E965 1995. URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500092.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500092.pdf.

Bellare:1995:PSS

[BR95b] M. Bellare and P. Rogaway. Provably secure session key distribution: The three party case. In ACM [ACM95], pages 57–66. ISBN 0-89791-718-9. LCCN QA 76.6 A13 1995. ACM order no. 508950.

Baldwin:1996:RRR

[BR96a] R. Baldwin and R. Rivest. RFC 2040: The RC5, RC5-CBC, RC5-CBC-pad, and RC5-CTS algorithms, October 1996. URL ftp://ftp.internic.net/rfc/rfc2040.txt; https://www.math.utah.edu/pub/rfc/rfc2040.txt. Status: INFORMATIONAL.

Bellare:1996:TCA

[BR96b] Mihir Bellare and Ronald L. Rivest. Translucent cryptography: an alternative to key escrow and its implementation via fractional oblivious transfer. Technical report MIT/LCS/TR-683, Massachusetts Institute of Technology. Laboratory for Computer Science, Cambridge, MA, USA, February 1996. 20 pp.

Bellare:1996:ESD

[BR96c] Mihir Bellare and Phillip Rogaway. The exact security of digital signatures — how to sign with RSA and Rabin. *Lecture Notes in Computer Science*, 1070: 399–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700399.htm; http://link.springer-ny.com/link/service/series/0558/papers/1070/10700399.pdf.

Bella:1997:FAK

[BR97a] G. Bella and E. Riccobene. Formal analysis of the Kerberos authentication system. *J.UCS: Journal of Universal Computer Science*, 3(12):1337–??, December 28, 1997. ISSN 0948-6968. URL http://medoc.springer.de:8000/jucs/jucs_3_12/formal_analysis_of_the.

Bellare:1997:MUR

[BR97b] M. Bellare and P. Rogaway. Minimizing the use of random oracles in authenticated encryption schemes. *Lecture Notes in Computer Science*, 1334:1–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1999:CVC

[BR99a] M. Bellare and P. Rogaway. On the construction of variable-input-length ciphers. In Knudsen [Knu99c], pages 231–244. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Bellare:1999:CVI

[BR99b] M. Bellare and P. Rogaway. On the construction of variable-input-length ciphers. *Lecture Notes in Computer Science*, 1636: 231–244, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Branstad:1975:DGI

[Bra75a] D. K. Branstad. Draft guidelines for implementing and using the NBS Data Encryption Standard. Report ??, U.S. National Bureau of Standards, Gaithersburg, MD, USA, November 10, 1975.

Branstad:1975:EPC

[Bra75b] D. K. Branstad. Encryption protection in computer data communications,. In ????, editor, *Fourth Data Communications Symposium, 7–9 October 1975, Quebec City, Canada*, page ?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1975.

Branstad:1979:VHD

[Bra79] D. Branstad. V. 'Hellman's data does not support his conclusion'. *IEEE Spectrum*, 16(7):41, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Brassard:1981:TLT

[Bra81] Gilles Brassard. A time-luck tradeoff in relativized cryptography. *Journal of Computer and System Sciences*, 22(3):280–311, June 1981. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0022000081900349`.

Bracha:1987:ERR

[Bra87a] Gabriel Bracha. An $O(\log n)$ expected rounds randomized Byzantine generals protocol. *Journal of the Association for Computing Machinery*, 34(4):910–920, October 1987. CODEN JACOAH. ISSN 0004-5411. URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/42229.html`.

Brassard:1987:IMC

[Bra87b] Gilles Brassard. Introduction to modern cryptology. Publication 606, Université de Montreal, Dèpartement d'Informatique et de Recherche Opèrationnelle, Montréal, Québec, Canada, 1987. 56 pp.

Brassard:1988:MCT

[Bra88] Gilles Brassard. *Modern cryptology: a tutorial*, volume 325 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-96842-3. ISSN 0302-9743 (print), 1611-3349 (electronic). vi + 107 pp. LCCN Z103 .B721 1988. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0325.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=325`.

Brassard:1989:CCb

[Bra89a] G. Brassard. Cryptology — column 2. *ACM SIGACT News*, 20(4):13, November 1989. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Brassard:1989:CCa

[Bra89b] Gilles Brassard. Cryptology column. *ACM SIGACT News*, 20(3):15–19, July 1989. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Brand:1990:PNU

[Bra90a] Russell L. Brand. Problems with the normal use of cryptography for providing security on unclassified networks (invited). *Lecture Notes in Computer Science*, 435:30–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350030.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350030.pdf.

Brasard:1990:CCH

[Bra90b] Gilles Brasard. Cryptology — column 3 hot news on interactive protocols. *ACM SIGACT News*, 21(1): 7, January 1990. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Brassard:1990:ACC

[Bra90c] Gilles Brassard, editor. *Advances in Cryptology — CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. CODEN LNCSD9. ISBN 0-387-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Brassard:1990:CCH

[Bra90d] Gilles Brassard. Cryptology — column 4: hiding information from oracles. *ACM SIGACT News*, 21(2): 5, Spring 1990. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Branstad:1993:RNW

[Bra93a] Dennis K. Branstad. Report of the NIST workshop on digital signature certificate mangement: December 10–11, 1992. Technical Report NIST 5234, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, October 1993. various pp.

Brassard:1993:CM

[Bra93b] Gilles Brassard. *Cryptologie moderne*, volume 9 of *Logique Mathematiques Informatique*. Masson Editeur, Masson, France, 1993. ISBN 2-225-83970-0. x + 124 pp. LCCN ???? Traduction de *Modern Cryptology*, Claude Goutier, traducteur.

Brassard:1994:CCQ

[Bra94a] Gilles Brassard. Cryptology column – quantum computing: The end of classical cryptography? *ACM SIGACT News*, 25(4):15–21, December 1994. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Bray:1994:UA

[Bra94b] Jeffrey K. Bray, editor. *Ultra in the Atlantic*, volume 11–16 of *An intelligence series*. Aegean Park Press, Laguna Hills, CA, USA, revised edition, 1994. ISBN 0-89412-235-5 (vol. 1), 0-89412-236-3 (vol. 2), 0-89412-237-1 (vol. 3), 0-89412-238-X (vol. 4), 0-89412-240-1 (vol. 5), 0-89412-241-X (vol. 6). ???? pp. LCCN D810.C88 U48 1994.

Brackin:1995:DCP

[Bra95a] S. H. Brackin. Deciding cryptographic protocol adequacy with HOL. *Lecture Notes in Computer Science*, 971:90–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brands:1995:LEC

[Bra95b] S. Brands. Off-line electronic cash based on secret-key certificates. *Lecture Notes in Computer Science*, 911:131–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brands:1995:RBS

[Bra95c] Stefan Brands. Restrictive blinding of secret-key certificates. *Lecture Notes in Computer Science*, 921:231–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210231.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0921/09210231.pdf`.

Brassard:1995:CCB

[Bra95d] Gilles Brassard. Cryptology Column: The Book I've Always Wanted To Write (almost). *ACM SIGACT News*, 26(2):18–20, June 1995. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Brassard:1995:IDR

[Bra95e] Gilles Brassard. The impending demise of RSA? *CryptoBytes*, 1(1):1, 3–4, Spring 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n1.pdf`.

Brackin:1996:DCP

[Bra96] S. H. Brackin. Deciding cryptographic protocol adequacy with HOL: The implementation. *Lecture Notes in Computer Science*, 1125:61–76, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brassard:1998:C

[Bra98] G. Brassard. Crypto '89. *Lecture Notes in Computer Science*, 1440: 101–110, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Breitrose:1997:ALD

[Bre97a] Charlie Breitrose. American legislators debate encryption laws. *Network Security*, 1997(7):9–10, July 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897898790.

Breitrose:1997:DEM

[Bre97b] Charlie Breitrose. Distributing encrypted messages more securely. *Network Security*, 1997(9):7, September 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348589780253X.

Brent:1999:CAP

[Bre99] Richard P. Brent. Computer arithmetic — a programmer's perspective. In Koren and Kornerup [KK99b], page 2. ISBN 0-7803-5609-8, 0-7695-0116-8, 0-7695-0118-4. ISSN 1063-6889. LCCN QA76.6 .S887 1999. URL http://euler.ecs.umass.edu/paper/final/brentr.pdf; http://euler.ecs.umass.edu/paper/final/brentr.ps; http://www.acsel-lab.com/arithmetic/arith14/papers/ARITH14_Brent.pdf. IEEE Computer Society Order Number PR00116. IEEE Order Plan Catalog Number 99CB36336.

Brickell:1985:BIK

[Bri85] Ernest F. Brickell. Breaking iterated knapsacks. In Blakley and Chaum [BC85], pages 342–358. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=342. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Brickell:1986:CKC

[Bri86] Ernest F. Brickell. The cryptanalysis of knapsack cryptosystems. In Ringeisen and Roberts [RR86], pages 3–23. ISBN 0-89871-219-X. LCCN QA76.9.M35C65 1986.

Brickell:1988:CKC

[Bri88] Ernest F. Brickell. The cryptanalysis of knapsack cryptosystems. In *Applications of discrete mathematics (Clemson, SC, 1986)*, pages 3–23. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1988.

Brickell:1990:SIS

[Bri90a] Ernest F. Brickell. Some ideal secret sharing schemes. *Lecture Notes in Computer Science*, 434:468–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340468.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340468.pdf`.

Brickell:1990:SHI

[Bri90b] Ernest F. Brickell. A survey of hardware implementations of RSA (invited), (abstract). *Lecture Notes in Computer Science*, 435: 368–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350368.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350368.pdf`.

Brickell:1992:ACC

[Bri92] Ernest F. Brickell, editor. *Advances in Cryptology–CRYPTO '92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992: Proceedings*, volume 740 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). LCCN QA76.9.A25 C79 1992. DM104.00.

Brickell:1993:ACC

[Bri93] Ernest F. Brickell, editor. *Advances in Cryptology — CRYPTO '92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992: Proceedings*, volume 740 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. CODEN LNCSD9. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1992. DM104.00.

Brickell:1998:C

[Bri98] E. F. Brickell. Crypto '92. *Lecture Notes in Computer Science*, 1440: 147–152, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brown:1975:BL

[Bro75] Anthony Cave Brown. *Bodyguard of lies*. Harper & Row, New York, NY, USA, 1975. ISBN 0-06-010551-8. x + 947 + 8 pp. LCCN D810.S7 C36 1975.

Brownell:1981:ODN

[Bro81] George A. Brownell. *The origin and development of the National Security Agency*, volume 35 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1981. ISBN 0-89412-054-9. x + 98 pp. LCCN UB290 .B76 1981. Edited by Wayne G. Barker. Originally published as report of the Ad hoc Committee to Study the Communications Intelligence Activities of the United States, George A. Brownell, chairman.

Brooke:1986:BRB

[Bro86] N. Michael Brooke. Book review: *Mr. Babbage's secret: the tale of a Cypher — and APL*: O. I. Franksen. Strandbergs Forlag, Denmark (1984). 320 pp. Dkr. 320.00. ISBN: 87-872-0086-4. *Information Processing and Management*, 22(1):67–68, ???? 1986. CODEN IPMADK. ISSN 0306-4573 (print), 1873-5371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/030645738690018X`.

Browne:1994:ECL

[Bro94] R. Browne. An entropy conservation law for testing the completeness of covert channel analysis. In ACM [ACM94a], pages 270–281. ISBN 0-89791-732-4. LCCN QA 76.9 A25 A26 1994. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/041205.html`.

Brock:1996:CCP

[Bro96] Steven G. (Steven Gary) Brock. The Clipper chip: policy perspectives on encryption, security, and privacy. Thesis (M.A.), University of Colorado, Boulder, CO, USA, 1996. v + 125 pp.

Brown:1997:JBC

[Bro97] Peter Brown. Java 16-bit cards: Sun, Siemens in Java/Smart Card pact. *Electronic News*, 43(2178): 14, July 28, 1997. CODEN ELNEAU. ISSN 0013-4937, 1061-6624.

Benedikt:1999:DLD

[BRS99] M. Benedikt, T. Reps, and M. Sagiv. A decidable logic for describing linked data structures. *Lecture Notes in Computer Science*, 1576:2–19, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bruyere:1991:MCB

[Bru91] V. Bruyere. Maximal codes with bounded deciphering delay. *Theoretical Computer Science*, 84(1):53–76, July 22, 1991. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Brundrett:1998:KAW

[Bru98] Peter Brundrett. Kerberos authentication in Windows NT 5.0 domains. *;login: the USENIX Association newsletter*, 23(3):??, May 1998. CODEN LOGNEM. ISSN 1044-6397. URL `http://www.usenix.org/publications/login/1998-5/brundrett.html`. Special issue on security.

Bentley:1999:SOE

[BRW99] Damian Bentley, Greg Rose, and Tara Whalen. `ssmail`: Opportunistic encryption in `sendmail`. In USENIX [USE99b], page ?? ISBN 1-880446-25-1. LCCN ???? URL `http://db.usenix.org/publications/library/proceedings/lisa99/bentley.html`.

Bryan:1967:CA

[Bry67] William G. Bryan. *Cryptographic ABC's*. Practical cryptanalysis; v. 4, 5. American Cryptogram Association, Greenfield, MA, USA, 1967.

Brillhart:1967:SFR

[BS67] John Brillhart and J. L. Selfridge. Some factorizations of $2^n \pm 1$ and related results. *Mathematics of Computation*, 21(97):87–96, January 1967. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Branstad:1982:ISS

[BS82] Dennis K. Branstad and Miles E. Smid. Integrity and security standards based on cryptography. *Computers and Security*, 1(3):255–260, November 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://`

www.sciencedirect.com/science/article/pii/016740488290044X.

Brickell:1983:SRK

[BS83] Ernest F. Brickell and Gustavus J. Simmons. A status report on knapsack based public key cryptosystems. *Congressus Numerantium*, 37:3–72, 1983. ISSN 0384-9864.

Benois:1986:CSE

[BS86] Michèle Benois and Jacques Sakarovitch. On the complexity of some extended word problems defined by cancellation rules. *Information Processing Letters*, 23(6):281–287, December 3, 1986. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Biham:1990:DCD

[BS90a] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. Technical report CS90-16, Department of Computer Science, Weizmann Institute of Science, Rehovot, Israel, July 1990. 107 pp.

Brown:1990:DPT

[BS90b] Lawrence Brown and Jennifer Seberry. On the design of permutation P in DES type cryptosystems. *Lecture Notes in Computer Science*, 434:696–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340696.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340696.pdf.

Beth:1991:NEC

[BS91a] T. Beth and F. Schaefer. Nonsupersingular elliptic curves for public key cryptosystems. *Lecture Notes in Computer Science*, 547:316–327, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470316.htm; http://link.springer-ny.com/link/service/series/0558/papers/0547/05470316.pdf.

Beth:1991:NSE

[BS91b] Thomas Beth and F. Schaefer. Non supersingular elliptic curves for public key cryptosystems. *Lecture Notes in Computer Science*, 547:316–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470316.htm; http://link.springer-ny.com/link/service/series/

0558/papers/0547/05470316.pdf.

Biham:1991:DCD

[BS91c] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems (invited talk). *Lecture Notes in Computer Science*, 537:2–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1991:DCFb

[BS91d] E. Biham and A. Shamir. Differential cryptanalysis of Feal and *N*-hash. *Lecture Notes in Computer Science*, 547:1–16, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1991:DCFa

[BS91e] Eli Biham and Adi Shamir. Differential cryptanalysis of Feal and *N*-hash. Technical report CS91-17, Department of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel, October 1991. 34 pp.

Biham:1991:DCS

[BS91f] Eli Biham and Adi Shamir. Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. Technical report CS91-18, Department of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel, October 1991. 36 pp.

Brickell:1991:SIB

[BS91g] Ernest F. Brickell and Douglas R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes (extended abstract). *Lecture Notes in Computer Science*, 537:242–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370242.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370242.pdf.

Broscius:1991:EPH

[BS91h] Albert G. Broscius and Jonathan M. Smith. Exploiting parallelism in hardware implementation of the DES. *Lecture Notes in Computer Science*, 576:367–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760367.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760367.pdf.

Biham:1993:DCF

[BS93a] E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. *Lecture Notes in Computer Science*, 740:487–496, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biham:1993:DCD

[BS93b] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-97930-1 (New York), 3-540-97930-1 (Berlin). ix + 188 pp. LCCN QA76.9.A25 B54 1993.

Brassard:1994:SKR

[BS94] Gilles Brassard and Louis Salvail. Secret key reconciliation by public discussion. *Lecture Notes in Computer Science*, 765: 410–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650410.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650410.pdf`.

Blaze:1995:MBC

[BS95a] M. Blaze and B. Schneier. The MacGuffin block cipher algorithm. *Lecture Notes in Computer Science*, 1008:97–110, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/macguffin.html`.

Boneh:1995:CSF

[BS95b] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. In Coppersmith [Cop95d], pages 452–465. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/044805.html`. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Bose:1995:ATV

[BS95c] P. Bose and S. Surya. Architectural timing verification of CMOS RISC processors. *IBM Journal of Research and Development*, 39(1/2):113–129, January/March 1995. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http:`

//www.almaden.ibm.com/journal/rd39-1.html#twelve.

Bruckstein:1995:SSD

[BS95d] A. M. Bruckstein and D. Shaked. Skew symmetry detection via invariant signatures. *Lecture Notes in Computer Science*, 970:17–24, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brunnstein:1995:IPR

[BS95e] Klaus Brunnstein and Peter Paul Sint, editors. *Intellectual property rights and new technologies: proceedings of the KnowRight '95 Conference, Vienna, Austria, August 21-25, 1995*, volume 82 of *Schriftenreihe der Osterreichischen Computer Gesellschaft*. R. Oldenbourg, Vienna, Austria, 1995. ISBN 3-486-23483-8 (Oldenbourg, Munchen), 3-7029-0408-5 (Oldenbourg, Wien), 3-85403-082-7 (Osterr. Computer-Ges.), 3-85403-082-7 (Osterreichische Computer Ges.). LCCN KJ118.I5 K66 1995.

Biham:1997:DFA

[BS97a] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. *Lecture Notes in Computer Science*, 1294:513–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bramhill:1997:CCD

[BS97b] I. D. Bramhill and M. R. C. Sims. Challenges for copyright in a digital age. *BT Technology Journal*, 15(2):63–73, April 1997. CODEN BTJUEH. ISSN 0265-0193. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061105.html.

Boneh:1998:CSF

[BS98] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, 44(5):1897–1905, September 1998. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073805.html.

Baaleh:1999:AGA

[BS99a] A. I. Baaleh and A. F. Sakr. Application of genetic algorithms in power system stabilizer design. *Lecture Notes in Computer Science*, 1611:165–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1999:NEE

[BS99b] M. Bellare and A. Sahai. Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. In Wiener [Wie99], pages 519–536. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Bellare:1999:NME

[BS99c] Mihir Bellare and Amit Sahai. Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. *Lecture Notes in Computer Science*, 1666:519–536, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660519.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1666/16660519.pdf`.

Barreiro:1997:PKC

[BSB97] Ernesto Reinaldo Barreiro, Jorge Estrada Sarlabous, and Jorge Alejandro Piñeiro Barcelo. A public key cryptosystem based on Picard codes. In *IVth Symposium of Mathematics (Spanish) (Havana, 1997)*, pages 47–57. Inst. Cibern. Mat. Fís., Havana, 1997.

Bakhtiari:1995:APL

[BSN95] S. Bakhtiari and R. Safavi-Naini. Application of PVM to linear cryptanalysis. In Gray and Naghdy [GN95b], pages 278–279. ISBN 90-5199-196-7. LCCN ????

Bakhtiari:1996:PAK

[BSNP96a] S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk. On password-based authenticated key exchange using collisionful hash functions. *Lecture Notes in Computer Science*, 1172:299–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bakhtiari:1996:PBA

[BSNP96b] S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk. On password-based authenticated key exchange using collisionful hash functions. *Lecture Notes in Computer Science*, 1172:299–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bakhtiari:1997:MAC

[BSNP97] S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk. A message authentication code based on Latin squares. *Lecture Notes in Computer Science*, 1270:194–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blake:1999:ECC

[BSS99] Ian F. Blake, G. Seroussi, and Nigel P. Smart. *Elliptic* *curves in cryptography*, volume 265 of *London Mathematical Society lecture note series*. Cambridge University Press, New York, NY, USA, 1999. ISBN 0-521-65374-6 (paperback). xv + 204 pp. LCCN QA76.9.A25 B57 1999.

Bateman:1989:NMC

[BSW89] P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff, Jr. The new Mersenne conjecture. *American Mathematical Monthly*, 96(2):125–128, February 1989. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). See letter to the editor [Mul89b]. The authors state: NEW MERSENNE CONJECTURE. *If two of the following statements about an odd positive integer p are true, then the third one is also true. (a)* $p = 2^k \pm 1$ *or* $p = 4^k \pm 3$. *(b)* $M_p(= 2^p - 1)$ *is prime. (c)* $(2^p + 1)/3$ *is prime.*

Benaloh:1994:RFS

[BT94] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In ACM [ACM94c], pages 544–553. ISBN 0-89791-663-8. LCCN QA76 .A15 1994. URL http://www.acm.org/pubs/articles/proceedings/stoc/195058/p544-benaloh/p544-benaloh.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/195058/p544-benaloh/. ACM order no. 508930.

BT:1997:BEC

[BT97] BT. BT's ECCp-97 challenge submission to Certicom. Technical report, BT Advanced Communications Technology Centre, Adastral Park, Martlesham, Suffolk, UK, March 1997. URL http://www.labs.bt.com/projects/security/crackers/p-97.txt.

Barmawi:1998:AEK

[BTD98] Ari Moesriami Barmawi, Shingo Takada, and Norihisa Doi. Augmented encrypted key exchange using RSA encryption and confounder. *Transactions of the Information Processing Society of Japan*, 39(12):3324–3332, 1998. CODEN JSGRD5. ISSN 0387-5806.

Boney:1996:DWA

[BTH96] Laurence Boney, Ahmed H. Tewfik, and Khaled N. Hamdy. Digital watermarks for audio signals. In IEEE [IEE96b], pages 473–480. ISBN 0-8186-7436-9 (paperback), 0-8186-7438-5, 0-8186-7437-7 (microfiche). LCCN QA76.575.I623 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1036.html. IEEE Computer Society

Press order number PR07436. IEEE Order Plan catalog number 96TB100057.

Buck:1982:PCS

[Buc82] R. Creighton Buck. The public cryptography study group. *Computers and Security*, 1(3):249–254, November 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900438`.

Buchmann:1991:NTA

[Buc91a] J. Buchmann. Number theoretic algorithms and cryptology. *Lecture Notes in Computer Science*, 529: 16–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Buck:1991:MCT

[Buc91b] R. Creighton Buck. Modern cryptology: a tutorial (Gilles Brassard). *SIAM Review*, 33(3):487–??, September 1991. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Bucholtz:1995:EEC

[Buc95a] Chris Bucholtz. Encryption exports, Clipper policy criticized by consortium. *Network Security*, 1995(7): 9, July 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/1353485896897327`.

Bucholtz:1995:SCS

[Buc95b] Chris Bucholtz. Suit challenges status of cryptography as munition. *Network Security*, 1995(5): 9, May 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/1353485896897121`.

Budge:1922:RS

[Bud22] Sir E. A. Wallis (Ernest Alfred Wallis) Budge. *The Rosetta Stone*. British Museum Press, London, UK, 1922. 8 + 1 pp. LCCN PJ1531.R3 1913. Reprinted with revisions in 1935, 1950, and 1968.

Budge:1929:RSB

[Bud29] Sir E. A. Wallis(Ernest Alfred Wallis) Budge. *The Rosetta Stone in the British Museum: the Greek, Demotic and Hieroglyphic texts of the decree inscribed on the Rosetta Stone conferring additional honours on Ptolemy V. Epiphanes (203-181 B.C.) ...*. British Museum Press, London, UK, 1929. viii + 323 pp. LCCN PJ1531 .R3 1929. Reprinted with revisions in 1929, 1935, 1950, and 1968.

Budge:1976:RSB

[Bud76] Sir E. A. Wallis (Ernest Alfred Wallis) Budge. *The Rosetta stone in the British Museum: the Greek, demotic, and hieroglyphic texts of the decree inscribed on the Rosetta stone conferring additional honours on Ptolemy V Epiphanes (203-181 B.C.) with English translations and a short history of the decipherment of the Egyptian hieroglyphs, and an appendix containing translations of the stelae of San (Tanis) and Tall al-Maskhutah.* AMS Press, New York, NY, USA, 1976. ISBN 0-404-11362-1. 325 + 22 pp. LCCN PJ1531.R5 B8 1976.

Burchard:1981:NNF

[Bur81] Hank Burchard. News and notices: Finerman and Lee Receive ACM Awards; summer positions at Digital Computer Museum; CBI Fellowship 1982–1983; GMD activities in the history of computing; request for articles; Edwards speaks at Digital Computer Museum; exhibit of cipher machines. *Annals of the History of Computing*, 3(4):410–413, October/December 1981. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1981/pdf/a4410.pdf`.

Burton:1984:RPKa

[Bur84a] Charles E. Burton. RSA: a public key cryptography system part I. *Dr. Dobb's Journal of Software Tools*, 9 (3):16–??, March 1984. CODEN DDJOEB. ISSN 1044-789X.

Burton:1984:RPKb

[Bur84b] Charles E. Burton. RSA: a public key cryptography system part II. *Dr. Dobb's Journal of Software Tools*, 9 (4):32–??, April 1984. CODEN DDJOEB. ISSN 1044-789X.

Burton:1985:EAC

[Bur85] Charles E. Burton. An enhanced ADFGVX cipher system. *Dr. Dobb's Journal of Software Tools*, 10(2):48–??, February 1985. CODEN DDJOEB. ISSN 1044-789X.

Burnham:1988:DES

[Bur88] B. Burnham. DES (data encryption standard) cryptographic services designed for the DOE wide band communications network. *Computers and Security*, 7 (5):510, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740488890212X`.

Burmester:1994:CCK

[Bur94a] M. Burmester. Cryptanalysis of the Chang-Wu-Chen key distribution system. *Lecture Notes in Computer Science*, 765:440–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Burmester:1994:CCW

[Bur94b] Mike V. D. Burmester. Cryptanalysis of the Chang-Wu-Chen key distribution system. *Lecture Notes in Computer Science*, 765:440–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650440.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650440.pdf.

Burmester:1994:ROD

[Bur94c] Mike V. D. Burmester. On the risk of opening distributed keys. In Desmedt [Des94b], pages 308–317. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390308.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390308.pdf.

Burmester:1996:HSS

[Bur96] M. Burmester. Homomorphisms of secret sharing schemes: a tool for verifiable signature sharing. *Lecture Notes in Computer Science*, 1070:96–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Burke:1998:IHC

[Bur98a] Colin Burke. An introduction to an historic computer document: the 1946 Pendergass report — cryptanalysis and the digital computer. In Deavours et al. [DKK+98], pages 361–371. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Burke:1998:LER

[Bur98b] Ralph Erskine Colin Burke. Letters to the editor — re: Safford article. In Deavours et al. [DKK+98], pages 279–286. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Burke:1999:AAC

[Bur99] Colin Burke. Automating American cryptanalysis 1930–45: Marvelous machines, a bit too late. *Intelligence and National Security*, 14(1):18–??, 1999. ISSN 0268-4527 (print), 1743-9019 (electronic).

Busse:1996:UFE

[Bus96] Dale T. Busse. User friendly encryption. Thesis (M.S. in Computer Science), Department of Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1996. viii + 41 pp.

Buss:1997:BAC

[Bus97] Samuel R. Buss. Bounded arithmetic, cryptography and complexity. *Theoria*, 63(3):147–167, December 1997. CODEN THRAA5. ISSN 0040-5825 (print), 1755-2567 (electronic).

Brouwer:1982:NMK

[Bv82] Andries E. Brouwer and Peter van Emde Boas. A note on: "Master keys for group sharing" [Inform. Process. Lett. **12** (1981), no. 1, 23–25; MR 82d:94046] by D. E. Denning and F. B. Schneider. *Information Processing Letters*, 14(1):12–14, March 27, 1982. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [DS81].

Boneh:1996:HCM

[BV96] Dan Boneh and Ramarathnam Venkatesan. Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes. *Lecture Notes in Computer Science*, 1109:129–142, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090129.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090129.pdf; http://theory.stanford.edu/~dabo/papers/dhmsb.ps.gz.

Boneh:1997:RLC

[BV97] D. Boneh and R. Venkatesan. Rounding in lattices and its cryptographic applications. In ACM [ACM97b], pages 675–681. CODEN PAAAF2. ISBN 0-89871-390-0. LCCN ???? URL http://theory.stanford.edu/~dabo/papers/nonuniform.ps.gz.

Barros:1998:DWS

[BV98a] B. Barros and F. Verdejo. Designing workspaces to support collaborative learning. *Lecture Notes in Computer Science*, 1416: 668–677, 1998. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Blunk:1998:RPE

[BV98b] L. Blunk and J. Vollbrecht. RFC 2284: PPP extensible authentication protocol (EAP), March 1998. URL ftp://ftp.internic.net/rfc/rfc2284.txt; https://www.math.utah.edu/pub/rfc/rfc2284.txt. Status: PROPOSED STANDARD.

Boneh:1998:BRM

[BV98c] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA may not be equivalent to factoring (extended abstract). *Lecture Notes in Computer Science*, 1403: 59–71, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030059.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030059.pdf; http://theory.stanford.edu/~dabo/papers/no_rsa_red.ps.gz.

Briguglio:1999:PGF

[BVFD99] S. Briguglio, G. Vlad, G. Fogaccia, and B. Di Martino. Parallelization of gridless finite-size-particle plasma simulation codes. *Lecture Notes in Computer Science*, 1593:241–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beker:1985:KMS

[BW85] Henry Beker and Michael Walker. Key management for secure electronic funds transfer in a retail environment. In Blakley and Chaum [BC85], pages 401–410. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=401. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Biehl:1997:TVC

[BW97] I. Biehl and S. Wetzel. Traceable visual cryptography. *Lecture Notes in Computer Science*, 1334:61–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brandes:1998:UGL

[BW98] U. Brandes and D. Wagner. Using graph layout to visualize train interconnection data. *Lecture Notes in Computer Science*, 1547:44–56, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biryukov:1999:SA

[BW99] A. Biryukov and D. Wagner. Slide attacks. In Knudsen [Knu99c], pages 245–259. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Blake-Wilson:1998:EAA

[BWM98] S. Blake-Wilson and A. Menezes. Entity authentication and authenticated key transport protocols employing asymmetric techniques. *Lecture Notes in Computer Science*, 1361:137–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blake-Wilson:1999:ADH

[BWM99a] S. Blake-Wilson and A. Menezes. Authenticated Diffie–Hellman key agreement protocols. *Lecture Notes in Computer Science*, 1556:339–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blake-Wilson:1999:UKS

[BWM99b] S. Blake-Wilson and A. Menezes. Unknown key-share attacks on the station-to-station (STS) protocol. *Lecture Notes in Computer Science*, 1560:154–170, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Buchholz:1988:CQDc

[BWV+88] Werner Buchholz, Maurice V. Wilkes, Alfred W. Van Sinderen, C. J. Fern, Jr., and W. L. van der Poel. Comments, queries, and debate: Babbage and the Colossus; Babbage and Bowditch; Two Early European Computers; Early Dutch Computer. *Annals of the History of Computing*, 10(3):218–221, July/September 1988. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1988/pdf/a3218.pdf`; `http://www.computer.org/annals/an1988/a3218abs.htm`.

Boyd:1992:RDE

[BY92] Colin Boyd and Tong Lai Yu. Remarks on a data encryption scheme of Yu and Yu (letters). *Communications of the Association for Computing Machinery*, 35(6):24–25, June 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [YY91].

Bellare:1993:CCT

[BY93a] M. Bellare and M. Yung. Certifying cryptographic tools: The case of trapdoor permutations. *Lecture Notes in Computer Science*, 740:442–460, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beller:1993:BDK

[BY93b] M. J. Beller and Y. Yacobi. Batch Diffie–Hellman key agreement systems and their application to portable communications. *Lecture Notes in Computer Science*, 658:208–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beller:1993:BDH

[BY93c] Michael J. Beller and Yacov Yacobi. Batch Diffie–Hellman key agreement systems and their application to portable communications. *Lecture Notes in Computer Science*, 658: 208–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580208.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580208.pdf`.

CBEMA:1981:ANS

[CA81] Computer and Business Equipment Manufacturers Association and American National Standards Institute. *American National Standard Data Encryption Algorithm*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, December 30, 1981. 16 pp. LCCN ???? ANSI X3.92-1981.

CBEMA:1983:ANSb

[CA83a] Computer and Business Equipment Manufacturers Association and American National Standards Institute. American National Standard for Information Systems: Data Encryption Algorithm — modes of operation. ???? ANSI X3.106-1983, American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, May 16, 1983. 16 pp.

CBEMA:1983:ANSa

[CA83b] Computer and Business Equipment Manufacturers Association and American National Standards Institute. American National Standard for Information Systems: Data link encryption. ???? ANSI X3.105-1983, American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, May 16, 1983. 20 pp.

Cachin:1995:LSS

[Cac95a] C. Cachin. On-line secret

sharing. *Lecture Notes in Computer Science*, 1025: 190–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cachin:1995:OSS

[Cac95b] C. Cachin. On-line secret sharing. *Lecture Notes in Computer Science*, 1025: 190–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cachin:1998:ITM

[Cac98] Christian Cachin. An information-theoretic model for steganography. *Lecture Notes in Computer Science*, 1525:306–318, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250306.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1525/15250306.pdf`.

Cypher:1996:UAS

[CadHSV96] Robert Cypher, Friedhelm Meyer auf der Heide, Christian Scheideler, and Berthold Vöcking. Universal algorithms for store-and-forward and wormhole routing. In ACM [ACM96b], pages 356–365. ISBN 0-89791-785-5. LCCN QA 76.6 A13 1996. URL `http://www.acm.org/pubs/articles/proceedings/stoc/237814/p356-cypher/p356-cypher.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/237814/p356-cypher/`.

Caelli:1996:CKE

[Cae96a] W. Caelli. Commercial key escrow: An Australian perspective. *Lecture Notes in Computer Science*, 1029: 40–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Caelli:1996:CPF

[Cae96b] W. Caelli. Cryptography: Personal freedom and law enforcement — is it possible to get agreement? *Lecture Notes in Computer Science*, 1029:1–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cain:1996:TS

[Cai96] Adam Douglas Cain. Text steganography. Thesis (M.S.), University of Illinois at Urbana-Champaign, Urbana-Champaign, IL, USA, 1996. vii + 90 pp.

Calvocoressi:1980:TSU

[Cal80] Peter Calvocoressi. *Top secret ultra*. Pantheon Books, New York, NY, USA, 1980.

ISBN 0-394-51154-9. 132 pp. LCCN D810.C88C34 1980.

Callimahos:1989:TAZ

[Cal89] Lambros D. Callimahos. *Traffic Analysis and the Zendian Problem: an exercise in communications intelligence operations*. Aegean Park Press, Laguna Hills, CA, USA, 1989. ISBN 0-89412-162-6, 0-89412-161-8 (paperback). 256 pp. LCCN ????

Callimahos:1992:HC

[Cal92] Lambros D. Callimahos. A history of cryptology. *Cryptolog*, 19(3):23–35, June 1992. ISSN 0740-7602. URL `https://archive.org/download/cryptolog_125/cryptolog_125.pdf`.

Campaigne:1971:REC

[Cam71] H. H. Campaigne. Reviews: *Elementary Cryptanalysis — A Mathematical Approach*, by Abraham Sinkov. *American Mathematical Monthly*, 78(4):423, April 1971. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Campbell:1987:MBC

[Cam87] Q. G. Campbell. Meteor burst communications protocols — the history and role of computing technology in radio communication via meteor trails. Technical Report 246, University of Newcastle upon Tyne, Newcastle upon Tyne, UK, November 1987. ??–?? pp. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1007.html`.

Cammack:1988:MDE

[Cam88] William Ervin Cammack. Methods of data encryption and a random polygraphic cipher algorithm for ASCII files. Thesis, University of Southern Mississippi, Hattiesburg, MS, USA, 1988. vi + 108 pp.

Cao:1999:CAR

[Cao99] Zhen Fu Cao. A conic analogue of RSA cryptosystems and some improved RSA cryptosystems. *Heilongjiang Daxue Ziran Kexue Xuebao*, 16(4):15–18, 1999. ISSN 1001-7011.

Capecchi:1994:TGR

[Cap94] Mario R. Capecchi. Targeted gene replacement. *Scientific American*, 270 (3):52–?? (Intl. ed. 34–41), March 1994. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Carlet:1993:PBF

[Car93] C. Carlet. Partially-bent functions. *Lecture Notes in Computer Science*, 740:

280–291, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Carlsen:1994:OPA

[Car94] Ulf Carlsen. Optimal privacy and authentication on a portable communications system. *Operating Systems Review*, 28(3):16–23, July 1994. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Caronni:1995:AOR

[Car95] Germano Caronni. Assuring ownership rights for digital images. In Brüggermann and Gerhardt-Häckl [BGH95b], pages 251–263. ISBN 3-528-05483-2. LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1046.html`.

Carter:1996:BAP

[Car96] J. R. Carter. Breaking the Ada Privacy Act. *ACM SIGADA Ada Letters*, 16 (3):52–55, May/June 1996. CODEN AALEE5. ISSN 1094-3641 (print), 1557-9476 (electronic).

Carr:1997:WDA

[Car97a] J. Scott Carr. Watermarking in the digital age. *Telecommunications (Americas Edition)*, 31(12): 62–??, December 1997. CODEN TLCMDV. ISSN 0278-4831.

Carter:1997:BLC

[Car97b] F. L. Carter. The breaking of the Lorenz cipher: An introduction to the theory behind the operational role of "Colossus" at BP. *Lecture Notes in Computer Science*, 1355:74–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Carter:1997:CCC

[Car97c] Frank Carter. Codebreaking with the Colossus computer: an account of the methods used for finding the k-wheel settings. Technical report, Bletchley Park Trust, Bletchley Park, UK, 1997. ???? pp.

Carter:1998:CCC

[Car98] Frank Carter. Codebreaking with the Colossus computer: an introduction to the techniques used, together with their mathematical basis. Technical report, Bletchley Park Trust, Bletchley Park, UK, 1998. 24 pp.

Carasik:1999:USS

[Car99] Anne H. Carasik. *Unix Secure Shell*. McGraw-Hill tools series. McGraw-Hill, New York, NY, USA, 1999. ISBN 0-07-134933-2 (paperback). xxv + 339 pp. LCCN QA76.76.O63 C37294 1999.

Casson:1976:SAD

[Cas76] Lionel Casson. *The Story of Archaeological Decipherment, from Egyptian Hieroglyphs to Linear B* by Maurice Pope (review). *Technology and Culture*, 17(3): 530–531, July 1976. CODEN TECUA3. ISSN 0040-165X (print), 1097-3729 (electronic). URL https://muse.jhu.edu/pub/1/article/891767/pdf.

Caswell:1995:EDA

[Cas95] Deborah L. Caswell. An evolution of DCE authorization services. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 46(6):49–54, December 1995. CODEN HPJOAX. ISSN 0018-1153. URL http://www.hp.com/hpj/95dec/dec95_49.pdf; http://www.hp.com/hpj/toc-12-95.html.

Chren:1996:RDU

[CB96] W. A. Chren, Jr. and C. H. Brogdon. RSA decryption using the one-hot residue number system. In *IEEE 39th Midwest symposium on Circuits and Systems, 1996*, volume 1, pages 551–554. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. CODEN ???? ISSN ????

Clark:1981:ECC

[CC81] George C. Clark, Jr. and J. Bibb Cain. *Error-correction coding for digital communications*. Plenum Press, New York, NY, USA; London, UK, 1981. ISBN 0-306-40615-2. xii + 422 pp. LCCN TK5102.5 .C52.

Chen:1995:SIB

[CC95] Jonathan Jen-Rong Chen and Henry Ker-Chang Chang. Secure information broadcasting scheme using embedded locks. *International Journal of Computer Systems Science and Engineering*, 10(2):67–74, April 1995. CODEN CSSEEI. ISSN 0267-6192.

Canteaut:1998:NAF

[CC98] Anne Canteaut and Florent Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, 1998. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Cai:1999:LBPa

[CC99a] Jin-Yi Cai and Thomas W. Cusick. A lattice-based public-key cryptosystem. *Information and Computation*, 151(1-2):17–31, 1999.

CODEN INFCEC. ISSN 0890-5401 (print), 1090-2651 (electronic).

Cai:1999:LBPb

[CC99b] Jin-Yi Cai and Thomas W. Cusick. A lattice-based public-key cryptosystem. *Lecture Notes in Computer Science*, 1556:219–233, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chun:1999:DMT

[CC99c] H. W. Chun and S. H. C. Chan. The design of a multi-tiered bus timetabling system. *Lecture Notes in Computer Science*, 1611: 771–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1988:MUS

[CCD88] D. Chaum, C. Crepeau, and I. Damgård. Multiparty unconditionally secure protocols. In ACM [ACM88], pages 11–19. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order no. 508880.

Canteaut:1999:NCA

[CCD99] A. Canteaut, P. Charpin, and H. Dobbertin. A new characterization of almost bent functions. In Knudsen [Knu99c], pages 186–200. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Chen:1998:VIC

[CCH98] Tung-Shou Chen, Chin-Chen Chang, and Min-Shiang Hwang. A virtual image cryptosystem based upon vector quantization. *IEEE Transactions on Image Processing*, 7(10): 1485–1488, 1998. CODEN IIPRE4. ISSN 1057-7149 (print), 1941-0042 (electronic).

Carter:1995:DVD

[CCN95] G. Carter, A. Clark, and L. Nielsen. DESV-1: a variation of the data encryption standard (DES). *Lecture Notes in Computer Science*, 917:427–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Carlet:1998:CBF

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes, and Cryptography*, 15(2): 125–156, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Coppersmith:1985:AF

[CD85] D. Coppersmith and J. H. Davenport. An application of factoring. *Journal of Symbolic Computation*, 1(2):241–243, June 1985. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Chuang:1991:MER

[CD91] Chih-Chwen C. Chuang and James George Dunham. Matrix extensions of the RSA algorithm. *Lecture Notes in Computer Science*, 537:140–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370140.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370140.pdf`.

Cramer:1995:SSS

[CD95] R. Cramer and I. Damgaard. Secure signature schemes based on interactive protocols. *Lecture Notes in Computer Science*, 963:297–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cramer:1996:NGS

[CD96] Ronald Cramer and Ivan Bjerre Damgård. New generation of secure and practical RSA-Based signatures. *Lecture Notes in Computer Science*, 1109:173–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090173.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090173.pdf`.

Chapman:1997:HHS

[CD97] M. Chapman and G. Davida. Hiding the hidden: a software system for concealing ciphertext in innocuous text. In Han et al. [HOQ97], pages 335–345. CODEN LNCSD9. ISBN 3-540-63696-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I554 1997. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064119.html`.

Clark:1998:OHA

[CD98a] Andrew Clark and Ed Dawson. Optimisation heuristics for the automated cryptanalysis of classical ciphers. *J. Combin. Math. Combin. Comput.*, 28:63–86, 1998. ISSN 0835-3026. Papers in honour of Anne Penfold Street.

Cramer:1998:ZPF

[CD98b] R. Cramer and I. Damgaard. Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free? *Lecture Notes in Computer Science*, 1462: 424–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Curtin:1998:BFS

[CD98c] Matt Curtin and Justin Dolske. A brute force search of DES keyspace. *;login: the USENIX Association newsletter*, 23(3):??, May 1998. CODEN LOGNEM. ISSN 1044-6397. URL `http://www.usenix.org/publications/login/1998-5/curtin.html`. Special issue on security.

Compton:1999:PTC

[CD99] K. J. Compton and S. Dexter. Proof techniques for cryptographic protocols. *Lecture Notes in Computer Science*, 1644:25–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cramer:1999:EMC

[CDD+99] Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin. Efficient multiparty computations secure against an adaptive adversary. *Lecture Notes in Computer Science*, 1592:311–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920311.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1592/15920311.pdf`.

Cowie:1996:WWN

[CDEH+96] J. Cowie, B. Dodson, R. M. Elkenbracht-Huizing, A. K. Lenstra, P. L. Montgomery, and J. Zayer. A world wide number field sieve factoring record: On to 512 bits. In Kim and Matsumoto [KM96a], pages 382–394. CODEN LNCSD9. ISBN 3-540-61872-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5553 1996.

Congedo:1995:SRS

[CDFI95] G. Congedo, G. Dimauro, A. M. Forte, and S. Impedovo. Selecting reference signatures for on-line signature verification. *Lecture Notes in Computer Science*, 974:521–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Callas:1998:ROM

[CDFT98] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. RFC 2440: OpenPGP message format, November 1998. URL `ftp://ftp.internic.net/rfc/rfc2440.txt`; `https:/`

/www.math.utah.edu/pub/rfc/rfc2440.txt. Status: PROPOSED STANDARD.

Chang:1995:SCP

[CDG95] X. Chang, Z.-D. Dai, and G. Gong. Some cryptographic properties of exponential functions. *Lecture Notes in Computer Science*, 917:415–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Capocelli:1991:SSS

[CDGV91] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *Lecture Notes in Computer Science*, 576:101–113, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Carter:1998:KSI

[CDN98] G. Carter, E. Dawson, and L. Nielsen. Key schedules of iterative block ciphers. *Lecture Notes in Computer Science*, 1438:80–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Canetti:1997:DE

[CDNO97] Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky. Deniable encryption. In Kaliski [Kal97c], pages 90–104. CODEN LNCSD9. ISBN 3-540-63384-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1997. URL ftp://theory.lcs.mit.edu/pub/tcryptol/96-02r.ps; http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940090.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940090.pdf.

Chen:1995:PDP

[CDP95] L. Chen, I. B. Damgård, and T. P. Pedersen. Parallel divertibility of proofs of knowledge. *Lecture Notes in Computer Science*, 950: 140–155, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cramer:1994:PPK

[CDS94] Ronald Cramer, Ivan Bjerre Damgård, and Berry Schoenmakers. Proof of partial knowledge and simplified design of witness hiding protocols. In Desmedt [Des94b], pages 174–187. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390174.

htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390174.pdf.

Chaum:1986:CRN

[CE86] David Chaum and Jan-Hendrik Evertse. Cryptanalysis of DES with a reduced number of rounds: sequences of linear factors in block ciphers. *Lecture Notes in Computer Science*, 218:192–211, 1986. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Certicom:1997:EC

[Cer97] Certicom. ECC challenges. Technical report, Certicom, ????, 1997. URL http://www.certicom.com/chal/index.htm.

Chaum:1987:DPD

[CEvdGP87] David Chaum, Jan-Hendrik Everse, Jeroem van de Graaf, and René Peralta. Demonstrating possession of a discrete logarithm without revealing it. In Odlyzko [Odl87b], pages 200–212. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Chaum:1978:ICP

[CF78] D. L. Chaum and R. S. Fabry. Implementing capability-based protection using encryption. Technical Report UCB/ERL M78/46, University of California, Berkeley, Berkeley, CA, USA, 1978. i + 9 pp.

Christoffersson:1988:CUH

[CF88] Per Christoffersson and Viveke Fak. *Crypto users' handbook: a guide for implementors of cryptographic protection in computer systems*. Elsevier, Amsterdam, The Netherlands, 1988. ISBN 0-444-70484-1. vii + 93 pp. LCCN QA76.9.A25 C821 1988.

Crawford:1992:AS

[CF92] David J. Crawford and Philip E. Fox (ed.). The Autoscritcher and the Superscritcher. *IEEE Annals of the History of Computing*, 14(3):9–22, July–September 1992. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL http://dlib.computer.org/an/books/an1992/pdf/a3009.pdf; http://www.computer.org/annals/an1992/a3009abs.htm.

Coe:1995:DDC

[CF95] Diane E. Coe and Judith A. Furlong. Developing and deploying corporate cryptographic systems. In USENIX Association [USE95c], pages 137–146. ISBN 1-880446-74-X. LCCN HF5548.33. U84 1995(1).

Castelfranchi:1999:BMA

[CF99] C. Castelfranchi and R. Falcone. Basic mental attitudes of a collaborating agent: Cognitive primitives for MAS. *Lecture Notes in Computer Science*, 1647: 188–209, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chouinard:1996:ITA

[CFG96] Jean-Yves Chouinard, Paul Fortier, and T. Aaron Gulliver, editors. *Information theory and applications II: 4th Canadian workshop, Lac Delage, Quebec, Canada, May 28–30, 1995: selected papers*, volume 1133 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-61748-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN Q350 .I515 1996 Bar. Canadian Workshop on Information Theory.

Callas:1999:FUI

[CFGS99] J. Callas, J. Feigenbaum, D. Goldschlag, and E. Sawyer. Fair use, intellectual property, and the information economy (panel session summary). In Franklin [Fra99], pages 173–183. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Ceruzzi:1991:RCK

[CFK+91] Paul Ceruzzi, Kenneth Flamm, Peggy Aldrich Kidwell, Herbert R. J. Grosch, and John A. N. Lee. Reviews: Campbell-Kelly: ICL: A Business and Technical History; Aspray: Computing Before Computers; Watson and Petre: Father, Son & Co.; Asimov and Frenkel: Robots: Machines in Man's Image; McNeil: An Encyclopedia of the History of Technology; Byte: Fifteenth Anniversary Summit; Deavours and Kruh: The Turing Bombe: Was it Enough?; Pearcey: A History of Australian Computing; Aspray: The Origins of John von Neumann's Theory of Automata; Crossley and Henry: Thus Spake al-Khwarizmi: a Translation of the text of Cambridge University Library Ms. li.vi.5; Fauvel and

Gerdes: African Slave and Calculating Prodigy: Bicentenary of the Death of Thomas Fuller; Marling: Maestro of Many Keyboards [brief biography of Donald Knuth]. *Annals of the History of Computing*, 13(1):111–117, January/March 1991. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1991/pdf/a1111.pdf; http://www.computer.org/annals/an1991/a1111abs.htm.

Chor:1994:TT

[CFN94] Benny Chor, Amos Fiat, and Moni Naor. Tracing traitors. In Desmedt [Des94b], pages 257–270. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390257.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390257.pdf.

Coppersmith:1996:LRR

[CFPR96a] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter. Low-exponent RSA with related messages. *Lecture Notes in Computer Science*, 1070:1–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coppersmith:1996:LER

[CFPR96b] Don Coppersmith, Matthew Franklin, Jacques Patarin, and Michael Reiter. Low-exponent RSA with related messages. *Lecture Notes in Computer Science*, 1070:1–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1070/10700001.pdf.

Canetti:1997:CES

[CFS97] Ran Canetti, John Friedlander, and Igor E. Shparlinski. On certain exponential sums and the distribution of Diffie–Hellman triples. Research report RC 20915 (92645), IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, July 9, 1997. 19 pp.

Cramer:1996:MAS

[CFSY96] Ronald Cramer, Matthew Franklin, Berry Schoenmakers, and Moti Yung. Multi-authority secret-ballot elections with linear work. *Lecture Notes in Computer Science*, 1070:72–??, 1996.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700072.htm; http://link.springer-ny.com/link/service/series/0558/papers/1070/10700072.pdf.

Coppersmith:1975:GCA

[CG75] Don Coppersmith and Edna Grossman. Generators for certain alternating groups with applications to cryptography. *SIAM Journal on Applied Mathematics*, 29(4):624–627, December 1975. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Chor:1985:RRL

[CG85] Benny Chor and Oded Goldreich. RSA/Rabin least significant bits are $\frac{1}{2} + \frac{1}{\mathrm{poly}(\log N)}$ secure (extended abstract). In Blakley and Chaum [BC85], pages 303–313. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=303. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Cover:1987:OPC

[CG87] Thomas M. Cover and B. Gopinath, editors. *Open Problems in Communication and Computation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-96621-8. LCCN TK5102.5 .O243 1987. US$25.00.

Chor:1988:UBS

[CG88] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17 (2):230–261, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Catalano:1998:NES

[CG98] D. Catalano and R. Gennaro. New efficient and secure protocols for verifiable signature sharing and other applications. *Lecture Notes in Computer Science*, 1462:105–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Canetti:1999:ETP

[CG99] Ran Canetti and Shafi Goldwasser. An efficient *Threshold* public key cryptosystem secure against adaptive chosen ciphertext attack. *Lecture Notes in Computer Science*, 1592: 90–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920090.htm; http://link.springer-ny.com/link/service/series/0558/papers/1592/15920090.pdf.

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. URL http://www.oreilly.com/catalog/securityusability/.

Clark:1993:EMS

[CGB+93] R. K. Clark, I. B. Greenberg, P. K. Boucher, T. F. Lunt, P. G. Neumann, D. M. Wells, and E. D. Jensen. Effects of multilevel security on real-time applications. In IEEE [IEE93c], pages 120–129. ISBN 0-8186-4330-7. ISSN 1063-9527. LCCN QA76.9.A25 C6375 1993. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/031208.html. IEEE Computer Society Press order number 4330-02. IEEE catalog number 93TH0581-9.

Canetti:1999:AST

[CGJ+99] Ran Canetti, Rosario Gennaro, Stanisław Jarecki, Hugo Krawczyk, and Tal Rabin. Adaptive security for threshold cryptosystems. In Wiener [Wie99], pages 98–115. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Chen:1996:TAP

[CGM96] L. Chen, D. Gollmann, and C. Mitchell. Tailoring authentication protocols to match underlying mechanisms. *Lecture Notes in Computer Science*, 1172: 121–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chen:1997:KEM

[CGM97a] L. Chen, D. Gollmann, and C. J. Mitchell. Key escrow in mutually mistrusting domains. *Lecture Notes in Computer Science*, 1189: 139–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chen:1997:AUM

[CGM97b] Liqun Chen, Dieter Gollmann, and Chris J. Mitchell. Authentication using minimally trusted servers. *Operating Systems Review*, 31 (3):16–28, July 1997. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chor:1985:VSS

[CGMA85] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In IEEE [IEE85], pages 383–395 (or 335–344??). ISBN 0-8186-0644-4 (paperback), 0-8186-4644-6 (microfiche), 0-8186-8644-8 (hardcover). LCCN QA 76 S979 1985.

Chen:1997:SSR

[CGMW97] L. Chen, D. Gollmann, C. J. Mitchell, and P. Wild. Secret sharing with reusable polynomials. *Lecture Notes in Computer Science*, 1270: 183–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cramer:1997:SOE

[CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Fumy [Fum97], pages 103–118. CODEN LNCSD9. ISBN 3-540-62975-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1997. Sponsored by the International Association for Cryptologic Research (IACR).

Capocelli:1994:FAU

[CGV94] Renato M. Capocelli, Luisa Gargano, and Ugo Vaccaro. A fast algorithm for the unique decipherability of multivalued encodings. *Theoretical Computer Science*, 134(1):63–78, November 07, 1994. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1994&volume=134&issue=1&aid=1644`.

Canetti:1994:MSP

[CH94a] Ran Canetti and Amir Herzberg. Maintaining security in the presence of transient faults. In Desmedt

[Des94b], pages 425–438. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390425.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390425.pdf.

Clark:1994:BSP

[CH94b] Paul C. Clark and Lance J. Hoffman. BITS: A Smartcard protected operating system. *Communications of the Association for Computing Machinery*, 37(11): 66–70, November 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/188371.html.

Cai:1996:PEA

[CH96] Jin-Yi Cai and S. (Steve) Homer, editors. *Proceedings, Eleventh Annual IEEE Conference on Computational Complexity: May 24–27, 1996, Philadelphia, Pennsylvania*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN 0-8186-7386-9, 0-8186-7387-7. LCCN QA267 .S765 1996; QA267.7 .I34 1996. IEEE catalog number 96CB3591.

Carrel:1997:RIO

[CH97a] D. Carrel and D. Harkins. The resolution of ISAKMP with Oakley. Internet Draft draft-ietf-ipsec-isakmp-oakley-03.txt., March 1997.

Chang:1997:SAG

[CH97b] Chin-Chen Chang and Shin-Jia Hwang. A simple approach for generating RSA keys. *Information Processing Letters*, 63(1):19–21, July 30, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chen:1998:PFR

[CH98] Mark Chen and Eric Hughes. Protocol failures related to order of encryption and signature: Computation of discrete logarithms in RSA groups. *Lecture Notes in Computer Science*, 1438:238–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1438/14380238.htm; http://link.springer-ny.com/link/service/series/0558/papers/1438/14380238.pdf.

Corcoran:1999:SCB

[CH99a] David Sims David Corcoran and Bob Hillhouse. Smart cards and biometrics. *Linux Journal*, 59:??, March 1999. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Cordon:1999:AMD

[CH99b] O. Cordon and F. Herrera. ALM: a methodology for designing accurate linguistic models for intelligent data analysis. *Lecture Notes in Computer Science*, 1642:15–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1979:UEM

[Cha79] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Thesis (M.S. in Computer Science), University of California, Berkeley, Berkeley, CA, USA, June 1979.

Chaum:1981:UEM

[Cha81] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the Association for Computing Machinery*, 24 (2):84–88, February 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1019.html.

Chandler:1983:IMC

[Cha83a] W. W. Chandler. The installation and maintenance of Colossus. *Annals of the History of Computing*, 5(3):260–262, July/September 1983. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1983/pdf/a3260.pdf; http://www.computer.org/annals/an1983/a3260abs.htm.

Chaum:1983:BSU

[Cha83b] D. Chaum. Blind signatures for untraceable payments. In ????, editor, *Advances in Cryptology, Proceedings of CRYPTO 82*, pages 199–203. Plenum Press, New York, NY, USA; London, UK, 1983.

Chaum:1985:HKS

[Cha85a] David Chaum. How to keep a secret alive extensible partial key, key safeguarding, and threshold systems. In Blakley and Chaum [BC85], pages 481–485. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http:/

/www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=481. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Chaum:1985:NSC

[Cha85b] David Chaum. New secret codes can prevent a computerized big brother. In Blakley and Chaum [BC85], pages 432–433. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=432. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Chaum:1985:SIT

[Cha85c] David Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the Association for Computing Machinery*, 28(10):1030–1044, October 1985. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/4373.html; http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1022.html.

Chang:1986:DKL

[Cha86a] C. C. Chang. On the design of a key-lock-pair mechanism in information protection systems. *BIT*, 26(4):410–417, 1986. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Chapman:1986:NFS

[Cha86b] J. W. M. Chapman. No final solution: a survey of the cryptanalytical capabilities of German military agencies, 1926–35. *Intelligence and National Security*, 1(1):13–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Chaum:1990:SDA

[Cha90] David Chaum. The spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities. *Lec-*

ture Notes in Computer Science, 435:591–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350591.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350591.pdf`.

Chaum:1991:SCS

[Cha91] David Chaum, editor. *Smart card 2000: selected papers from the Second International Smart Card 2000 Conference, Amsterdam, The Netherlands, 4–6 October 1989*. North-Holland, Amsterdam, The Netherlands, 1991. ISBN 0-444-89266-4. LCCN TK7895.S62 I57 1989.

Chaum:1992:AEPb

[Cha92a] D. Chaum. Achieving electronic privacy. *Scientific American [International Edition]*, 267(2):76–81, August 1992. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Chaum:1992:AEPa

[Cha92b] David Chaum. Achieving electronic privacy. *Scientific American*, 267(2):96–?? (Intl. ed. 76–81), August 1992. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Chaum:1993:NCB

[Cha93] D. Chaum. Numbers can be a better form of cash than paper. *Lecture Notes in Computer Science*, 741: 174–178, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chambers:1994:TSC

[Cha94a] B. Chambers. Two stream ciphers. *Lecture Notes in Computer Science*, 809: 51–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chandler:1994:IAF

[Cha94b] James P. Chandler. Identification and analysis of foreign laws and regulations pertaining to the use of commercial encryption products for voice and data communications. Technical Report K/DSRD/SUB/93-RF105/3, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 1994. v + 10 pp.

Chabaud:1995:SSC

[Cha95a] Florent Chabaud. On the security of some cryptosystems based on error-correcting codes. *Lecture Notes in Computer Science*,

950:131–139, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1995:DCS

[Cha95b] D. Chaum. Designated confirmer signatures. *Lecture Notes in Computer Science*, 950:86–91, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1998:Cb

[Cha98] D. Chaum. Crypto '83. *Lecture Notes in Computer Science*, 1440:23–28, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chadwick:1999:IWS

[Cha99a] David Chadwick. Internet watch: Smart cards aren't always the smart choice. *Computer*, 32(12):142–143, December 1999. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co1999/pdf/rz142.pdf.

Chan:1999:WES

[Cha99b] Alvin T. S. Chan. Web-enabled smart card for ubiquitous access of patient's medical record. *Computer Networks (Amsterdam, Netherlands: 1999)*, 31(11–16):1591–1598, May 17, 1999. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.elsevier.com/cas/tree/store/comnet/sub/1999/31/11-16/2182.pdf.

Chau:1999:QCE

[Cha99c] H. F. Chau. Quantum convolutional error correction codes. *Lecture Notes in Computer Science*, 1509: 314–324, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chesson:1973:CC

[Che73] F. W. (Frederick William) Chesson. Computers and cryptology. *Datamation*, ?? (??):62–77, January 1973. CODEN DTMNAT. ISSN 0011-6963.

Cheswick:1992:EBW

[Che92] Bill Cheswick. An evening with Berferd in which a cracker is lured, endured, and studied. In USENIX [USE92a], pages 163–174.

Canetti:1997:MAC

[CHH97] R. Canetti, S. Halevi, and A. Herzberg. Maintaining authenticated communication in the presence of break-ins. In *Proc. 16th ACM Symp. on Principles of Distributed Computation*, page ?? ACM Press, New York, NY 10036, USA, 1997.

Chiopris:1992:SBE

[Chi92] Carlo Chiopris. The SECReTS banking expert system from phase 1 to phase 2. *Lecture Notes in Computer Science*, 636:91–??, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chin:1999:HCD

[Chi99a] Shiu-Kai Chin. High-confidence design for security: don't trust — verify. *Communications of the Association for Computing Machinery*, 42(7): 33–37, July 1999. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/cacm/1999-42-7/p33-chin/`.

Chin:1999:HDS

[Chi99b] Shiu-Kai Chin. High-confidence design for security: don't trust — verify. *Communications of the Association for Computing Machinery*, 42(7): 33–37, July 1999. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/cacm/1999-42-7/p33-chin/`.

Christophides:1999:ODI

[CHLT99] V. Christophides, C. Houstis, S. Lalis, and H. Tsalapata. Onthology-driven integration of scientific repositories. *Lecture Notes in Computer Science*, 1649: 190–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Canetti:1997:PSL

[CHN97] Ran Canetti, Amir Herzberg, and Dalit Naor. Proactive security: Long-term protection against break-ins. *CryptoBytes*, 3(1):1, 3–8, Spring 1997. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto3n1.pdf`.

Chor:1986:TIP

[Cho86] Ben-Zion Chor. *Two issues in public key cryptography: RSA bit security and a new knapsack type system*. ACM distinguished dissertations. MIT Press, Cambridge, MA, USA, 1986. ISBN 0-262-03121-3. 78 pp. LCCN TK5102.5 .C4781 1986. Originally presented as the author's thesis (doctoral — MIT, 1985).

Chung:1998:DWCb

[CHO+98] Tae-Yun Chung, Min-Suk Hong, Young-Nam Oh, Dong-Ho Shin, and Sang-Hui Park. Digital watermarking for copyright protection of MPEG2 compressed video. *IEEE Transactions on Consumer*

Electronics, 44(3):895–901, August 1998. CODEN ITCEDA. ISSN 0098-3063.

Christiansen:1978:SL

[Chr78] D. Christiansen. Spectral lines. *IEEE Spectrum*, 15 (1):23, January 1978. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Christoffersson:1988:MAE

[Chr88] Per Christoffersson. Message authentication and encryption combined. *Computers and Security*, 7(1): 65–71, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888905056.

Christianson:1998:SPI

[Chr98] Bruce Christianson, editor. *Security protocols: 5th international workshop, Paris, France, April 7–9, 1997: proceedings*, volume 1361 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. CODEN LNCSD9. ISBN 3-540-64040-1 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25S44 1998.

Christianson:1999:DSCb

[Chr99a] Bruce Christianson. Delegation and not-so smart card (transcript of discussion). *Lecture Notes in Computer Science*, 1550: 158–167, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1550/15500158.htm; http://link.springer-ny.com/link/service/series/0558/papers/1550/15500158.pdf.

Christianson:1999:SPI

[Chr99b] Bruce Christianson, editor. *Security protocols: 6th International Workshop, Cambridge, UK, April 15–17, 1998: Proceedings*, volume 1550 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. CODEN LNCSD9. ISBN 3-540-65663-4 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 S45 1999. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1550.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1550.

Chuang:1989:NES

[Chu89] Ta-Fu Chuang. *Non-homomorphic encryption schemes and properties of Chinese remainder theorem*. Thesis (Ph.D. in engineering), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1989. vi + 58 pp.

Currie:1996:SEL

[CI96] D. L. Currie and C. E. Irvine. Surmounting the effects of lossy compression on steganography. In Anonymous [Ano96a], pages 194–201. LCCN QA76.9.A25 N36 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054119.html`.

Ciarcia:1986:BHD

[Cia86] Steve Ciarcia. Build a hardware data encryptor. *BYTE Magazine*, 11(??):??, ?? 1986. CODEN BYTEDJ. ISSN 0360-5280.

Cao:1999:DTJ

[CIBM99] Y. J. Cao, N. Ireson, L. Bull, and R. Miles. Design of a traffic junction controller using classifier system and fuzzy logic. *Lecture Notes in Computer Science*, 1625:342–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Clark:1995:SRP

[CJ95] John Clark and Jeremy Jacob. On the security of recent protocols. *Information Processing Letters*, 56 (3):151–155, November 10, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chabaud:1998:DCS

[CJ98] F. Chabaud and A. Joux. Differential collisions in SHA-0. *Lecture Notes in Computer Science*, 1462: 56–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Collins:1999:DCL

[CJ99] Francis S. Collins and Karin G. Jegalian. Deciphering the code of life. *Scientific American*, 281 (6):86–??, December 1999. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Coster:1992:ILD

[CJL+92] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C. P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Computational complexity*, 2(??): 111–128, ???? 1992. CODEN CPTCEU. ISSN 1016-3328. URL `http://www.research.att.com/~amo/doc/arch/better.`

low.density.pdf; http://www.research.att.com/~amo/doc/arch/better.low.density.ps; http://www.research.att.com/~amo/doc/arch/better.low.density.tex.

Coppersmith:1995:TCB

[CJM95] Don Coppersmith, Don B. Johnson, and Stephen M. Matyas. Triple DES cipher block chaining with output feedback masking. Sent to ANSI., 1995.

Coppersmith:1996:PMT

[CJM96] D. Coppersmith, D. B. Johnson, and S. M. Matyas. A proposed mode for triple DES encryption. *IBM Journal of Research and Development*, 40(2):253–262, March 1996. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL http://www.almaden.ibm.com/journal/rd40-2.html#seven.

Charlwood:1998:EXA

[CJR98a] S. Charlwood and P. James-Roxby. Evaluation of the XC6200-series architecture for cryptographic applications. *Lecture Notes in Computer Science*, 1482: 218–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Charlwood:1998:EXS

[CJR98b] S. Charlwood and P. James-Roxby. Evaluation of the XC6200-series architecture for cryptographic applications. *Lecture Notes in Computer Science*, 1482: 218–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chari:1999:TSA

[CJRR99a] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Wiener [Wie99], pages 398–412. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Chari:1999:CNR

[CJRR99b] Suresh Chari, Charanjit Jutla, Josyula Rao, and Pankaj Rohatgi. A cautionary note regarding evaluation of AES candidates on smart-cards. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://citeseer.nj.nec.com/chari99cautionary.html; http://csrc.nist.gov/encryption/aes/round1/conf2/papers/chari.pdf. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

Chee:1991:CNP

[CJS91] Yeow Meng Chee, Antoine Joux, and Jacques Stern. The cryptanalysis of a new public-key cryptosystem based on modular knapsacks. *Lecture Notes in Computer Science*, 576:204–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760204.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760204.pdf`.

Chor:1990:SSI

[CK90] Benny Chor and Eyal Kushilevitz. Secret sharing over infinite domains (extended abstract). *Lecture Notes in Computer Science*, 435:299–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350299.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350299.pdf`.

Chor:1993:CPT

[CK93] Benny Chor and Eyal Kushilevitz. A communication-privacy tradeoff for modular addition. *Information Processing Letters*, 45(4):205–210, March 22, 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Cole:1995:MDR

[CK95] P. A. R. Cole and M. S. Khan. Modelling 3-D rigid solid objects using the view signature II representation scheme. *Lecture Notes in Computer Science*, 970:154–161, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chor:1998:PIR

[CKGS98] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *Journal of the Association for Computing Machinery*, 45(6):965–981, November 1998. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org:80/pubs/citations/journals/jacm/1998-45-6/p965-chor/`.

Cox:1996:SRW

[CKLS96a] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon.

A secure, robust watermark for multimedia. In Anderson [And96c], pages 185–206. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054118.html`.

Cox:1996:SIY

[CKLS96b] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure, imperceptible yet perceptually salient, spread spectrum watermark for multimedia. In IEEE [IEE96f], pages 192–197. CODEN SCOREX. ISBN 0-7803-3268-7 (softbound), 0-7803-3269-5 (casebound). LCCN TK 7801 S68 1996. IEEE catalog number 96CB35925.

Cox:1996:SSS

[CKLS96c] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure spread spectrum watermarking for images, audio and video. In IEEE [IEE96e], pages 243–246. ISBN 0-7803-3258-X (softbound), 0-7803-3259-8 (casebound), 0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM). LCCN TK8315.I222 1996. IEEE catalog number 96CH35919.

Cox:1997:SSS

[CKLS97] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12): 1673–1687, December 1997. CODEN IIPRE4. ISSN 1057-7149 (print), 1941-0042 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/071112.html`.

Caldwell:1999:DIF

[CKM99] A. E. Caldwell, A. B. Kahng, and I. L. Markov. Design and implementation of the Fiduccia-Mattheyses heuristic for VLSI netlist partitioning. *Lecture Notes in Computer Science*, 1619: 177–193, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coradeschi:1999:IVD

[CKN99] S. Coradeschi, L. Karlsson, and K. Nordberg. Integration of vision and decision-making in an autonomous airborne vehicle for traffic surveillance. *Lecture Notes in Computer Science*, 1542: 216–230, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chan:1988:IEC

[CL88] Yeng Kit Chan and Rudolf Lidl. On implementing elliptic curve cryptosystems. In *Contributions to general algebra, 6*, pages 155–166. Hölder-Pichler-Tempsky, Vienna, 1988.

Chang:1997:PCM

[CL97a] Chin-Chen Chang and Der-Chyuan Lou. Parallel computation of the multi-exponentiation for cryptosystems. *International Journal of Computer Mathematics*, 63(1-2):9–26, 1997. CODEN IJCMAT. ISSN 0020-7160.

Cox:1997:PWR

[CL97b] I. J. Cox and J. P. M. G. Linnartz. Public watermarks and resistance to tampering. In IEEE [IEE97j], page ?? ISBN 0-8186-8183-7 (paperback), 0-8186-8184-5 (casebound), 0-8186-8185-3 (microfiche). LCCN TK8315 .I16 1997. URL ftp://ftp.nj.nec.com/pub/ingemar/papers/icip97.ps; http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1049.html. Three volumes. IEEE order plan catalog number 97CB36144.

Cox:1998:SGM

[CL98] I. J. Cox and J. P. M. G. Linnartz. Some general methods for tampering with watermarks. *IEEE Journal on Selected Areas in Communications*, 16(4):587–593, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072113.html.

Claudy:1912:TMS

[Cla12] C. H. Claudy. A triple mirror for secret signaling. *Scientific American*, 107(17):346, October 26, 1912. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v107/n17/pdf/scientificamerican10261912-346.pdf.

Clark:1977:MWBa

[Cla77a] Ronald William Clark. *The man who broke Purple: the life of Colonel William F. Friedman, who deciphered the Japanese code in World War II.* Little, Brown, Boston, MA, USA, 1977. ISBN 0-316-14595-5. ix + 271 pp. LCCN UB290 .C58 1977.

Clark:1977:MWBb

[Cla77b] Ronald William Clark. *The man who broke Purple: the life of the world's greatest cryptologist, Colonel William F. Friedman.* Weidenfeld and Nicolson, London, UK, 1977. ISBN 0-297-77279-1. xi + 212 + 4 pp. LCCN UB290 .C58 1977b.

Clapp:1997:OFS

[Cla97] C. S. K. Clapp. Optimizing a fast stream cipher for VLIW, SIMD, and superscalar processors. *Lecture Notes in Computer Science*, 1267:273–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Clapp:1998:JHS

[Cla98a] C. S. K. Clapp. Joint hardware / software design of a fast stream cipher. *Lecture Notes in Computer Science*, 1372:75–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Clark:1998:TIT

[Cla98b] A. Clark. Too intelligent, or too artificial, or both? [book reviews]. *IEEE Spectrum*, 35(10):12–14, October 1998. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Clarke:1998:BP

[Cla98c] William F. Clarke. Bletchley Park 1941–1945. In Deavours et al. [DKK+98], pages 227–234. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Clapp:1999:ILP

[Cla99] Craig Clapp. Instruction-level parallelism in AES candidates. In National Institute of Standards and Technology [Nat99b], page 16. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf2/Clapp.pdf`. Only the slides for the conference talk are available.

Cleve:1991:CTI

[Cle91] R. Cleve. Complexity theoretic issues concerning block ciphers related to D.E.S. *Lecture Notes in Computer Science*, 537:530–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Clevenger:1996:DEU

[Cle96] Mark Allen Clevenger. Data encryption using RSA public-key cryptosystem. Thesis (M.S.), Ball State University, Muncie, IN, USA, 1996. ii + 149 pp.

Chang:1998:SOM

[CLHL98] Chin-Chen Chang, Jyh-Jong Leu, Pai-Cheng Huang, and Wei-Bin Lee. A scheme for obtaining a message from the digital multisignature. *Lecture Notes in Computer Science*, 1431: 154–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310154.htm; http://link.springer-ny.com/link/service/series/0558/papers/1431/14310154.pdf`.

Clinton:1997:AEC

[Cli97] Bill Clinton. *Administration of export controls on encryption products: communication from the President of the United States transmitting revisions to the provisions that apply to the Department of Commerce in the Export Administration regulations, 15 CFR part 730 et seq. — received in the United States House of Representatives November 15, 1996, pursuant to 50 U.S.C. 1703(b)*. Washington, DC, USA, January 7, 1997. 5 pp. Referred to the Committee on International Relations. Shipping list no.: 97-0126-P.

Clinton:1999:LPM

[Cli99] Bill Clinton. *A legislative proposal: message from the President of the United States transmitting a legislative proposal to protect the privacy, security and safety of the people of the United States through support for the widespread use of encryption, protection of the security of cryptographic keys, and facilitation of access to the plaintext of data for legitimate law enforcement purposes*. United States Government Printing Office, Washington, DC, USA, September 21, 1999. 40 pp. Referred to the Committee on the Judiciary and Government Reform. Shipping list no.: 2000-0018-P.

Chua:1999:ART

[CLL99] Seng Kiat Chua, Ka Hin Leung, and San Ling. Attack on RSA-type cryptosystems based on singular cubic curves over $\boldsymbol{Z}/\boldsymbol{nZ}$. *Theoretical Computer Science*, 226(1–2):19–27, September 17, 1999. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1999&volume=226&issue=1-2&aid=3223`.

Cheng:1998:MVR

[CLW98] Yi Chang Cheng, Erl Huei Lu, and Shaw Woei Wu. A modified version of the Rao–Nam algebraic-code encryption scheme. *Information Processing Letters*, 68(4):215–217, November 30, 1998. CODEN IF-

PLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Culik:1979:SIS

[CM79] K. Culik, II and H. A. Maurer. Secure information storage and retrieval using new results in cryptography. *Information Processing Letters*, 8(4):181–186, April 30, 1979. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ciampi:1982:EVS

[CM82] Constantino Ciampi and A. A. Martino, editors. *Edited versions of selected papers from the International Conference on "Logic, Informatics, Law," Florence, Italy, April 6–10, 1981*. Elsevier Science Publishers, Amsterdam, The Netherlands, 1982. ISBN 0-444-86413-X (set), 0-444-86414-8 (vol. 1), 0-444-86415-6 (vol. 2). LCCN K662.I4 I58. Two volumes. Vol. 1: Artificial intelligence and legal information systems. Vol. 2: Deontic logic, computational linguistics, and legal information systems.

Chan:1985:NMP

[CM85] B. Chan and H. Meijer. A note on the method of puzzles for key distribution. *International Journal of Computer and Information Sciences*, 14(4):221–223, August 1985. CODEN IJCIAH. ISSN 0091-7036.

Cachin:1995:LIR

[CM95] C. Cachin and U. M. Maurer. Linking information reconciliation and privacy amplification. *Lecture Notes in Computer Science*, 950: 266–274, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Callahan:1996:AVV

[CM96] John R. Callahan and Todd L. Montgomery. An approach to verification and validation of a reliable multicasting protocol. *ACM SIGSOFT Software Engineering Notes*, 21(3):187–194, May 1996. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Cachin:1997:USA

[CM97a] Christian Cachin and Ueli M. Maurer. Unconditional security against memory-bounded adversaries. *Lecture Notes in Computer Science*, 1294:292–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940292.htm`; `http://link.springer-`

ny.com/link/service/series/0558/papers/1294/12940292.pdf.

Chang:1997:CAS

[CM97b] L. W. Chang and I. S. Moskowitz. Critical analysis of security in voice hiding techniques. In Han et al. [HOQ97], pages 203–216. CODEN LNCSD9. ISBN 3-540-63696-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I554 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064118.html.

Cooperman:1997:SMD

[CM97c] Marc Cooperman and Scott A. Moskowitz. Steganographic method and device, March 18, 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1047.html. US Patent 5,613,004.

Cox:1997:RWI

[CM97d] Ingemar J. Cox and Matt L. Miller. A review of watermarking and the importance of perceptual modeling. In Rogowitz and Pappas [RP97b], pages 92–99. ISBN 0-8194-2427-7. LCCN TS510.S63 v.3016. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1045.html.

Chen:1998:DRT

[CM98] D. Chen and A. K. Mok. Design of a real-time SQL engine in the distributed environment. *Lecture Notes in Computer Science*, 1553: 27–38, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Camenisch:1999:SEG

[CM99a] J. Camenisch and M. Michels. Separability and efficiency for generic group signature schemes. In Wiener [Wie99], pages 413–430. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Charlton:1999:DPM

[CM99b] P. Charlton and E. Mamdani. A developer's perspective on mult-agent system design. *Lecture Notes in Computer Science*, 1647: 41–51, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Christianson:1999:DSCa

[CM99c] Bruce Christianson and James A. Malcolm. Delegation and not-so smart cards (position paper). *Lecture Notes in Computer Science*, 1550:154–157, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/

link/service/series/0558/bibs/1550/15500154.htm; http://link.springer-ny.com/link/service/series/0558/papers/1550/15500154.pdf.

Coradeschi:1999:HMC

[CM99d] S. Coradeschi and D. Malec. How to make a challenging al course enjoyable using the RoboCup soccer simulation system. *Lecture Notes in Computer Science*, 1604:120–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chen:1998:SCC

[CMKK98] Lily Chen, James L. Massey, Gurgen H. Khachatrian, and Melsik K. Kuregian. SAFER+: Cylink Corporation's submission for the Advanced Encryption Standard. In National Institute of Standards and Technology [Nat98], page 20. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf1/saferpls-slides.pdf. Only the slides for the conference talk are available.

Cohen:1993:AAA

[CMM93] G. Cohen, Teo Mora, and Oscar Moreno, editors. *Applied algebra, algebraic algorithms, and error-correcting codes: 10th International Symposium, AAECC-10, San Juan de Puerto Rico, Puerto Rico, May 10–14, 1993: proceedings*, volume 673 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. CODEN LNCSD9. ISBN 3-540-56686-4 (Berlin), 0-387-56686-4 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .A35 1993. DM72.00. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0673.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=673.

Canetti:1999:ECS

[CMN99] Ran Canetti, Tal Malkin, and Kobbi Nissim. Efficient communication-storage tradeoffs for multicast encryption. *Lecture Notes in Computer Science*, 1592:459–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920459.htm; http://link.springer-ny.com/link/service/series/0558/papers/1592/15920459.pdf.

Charnes:1997:SSH

[CMPS97] C. Charnes, K. Martin, J. Pieprzyk, and R. Safavi-Naini. Secret sharing in hierarchical groups. *Lecture Notes in Computer Science*, 1334:81–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chor:1989:SCT

[CMS89] Benny Chor, Michael Merritt, and David B. Shmoys. Simple constant-time consensus protocols in realistic failure models. *Journal of the Association for Computing Machinery*, 36(3):591–614, July 1989. CODEN JACOAH. ISSN 0004-5411. URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/65956.html. **Review: Computing Reviews**, June 1990.

Chuan-Ming:1994:RTR

[CMTNY94] Li Chuan-Ming, Hwang Tzonelih, and Lee Narn-Yih. Remark on the threshold RSA signature scheme. *Lecture Notes in Computer Science*, 773:413–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Craver:1997:CIW

[CMYY97] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Can invisible watermark resolve rightful ownerships? In Sethi and Jain [SJ97], pages 310–321. ISBN 0-8194-2433-1. LCCN TS510.S63 v.3022. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/063115.html.

Craver:1998:RRO

[CMYY98] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving rightful ownership with invisible watermarking techniques: Limitations, attacks and implications. *IEEE Journal on Selected Areas in Communications*, 16(4):573–586, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072114.html.

Crilly:1987:BPB

[CN87] Tony Crilly and Shekhar Nandy. The birthday problem for boys and girls. *The Mathematical Gazette*, 71(455):19–22, March 1987. CODEN MAGAAS. ISSN 0025-5572. URL http://links.jstor.org/sici?sici=0025-5572%28198703%292%3A71%3A455%3C19%3ATBPFBA%3E2.0.CO%3B2-7.

Coron:1999:SRSb

[CN99] Jean-Sébastien Coron and David Naccache. On the security of RSA screening. *Lecture Notes in Computer Science*, 1560: 197–203, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1560/15600197.htm; http://link.springer-ny.com/link/service/series/0558/papers/1560/15600197.pdf.

Coron:1999:SRP

[CNS99a] Jean-Sébastien Coron, David Naccache, and Julien P. Stern. On the security of RSA padding. In Wiener [Wie99], pages 1–18. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660001.pdf.

Coupe:1999:ELA

[CNS99b] Christophe Coupé, Phong Nguyen, and Jacques Stern. The effectiveness of lattice attacks against low-exponent RSA. *Lecture Notes in Computer Science*, 1560:204–218, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1560/15600204.htm; http://link.springer-ny.com/link/service/series/0558/papers/1560/15600204.pdf.

Chao:1998:CSE

[CNST98] Jinhui Chao, Osamu Nakamura, Kohji Sobataka, and Shigeo Tsujii. Construction of secure elliptic cryptosystems using CM tests and liftings. *Lecture Notes in Computer Science*, 1514: 95–109, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coltell:1998:AOL

[CO98] O. Coltell and J. M. Ordovas. Applying object logic programming to design computer strategies in gene scanning. *Lecture Notes in Computer Science*, 1416:619–627, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cocks:1997:SKG

[Coc97] C. Cocks. Split knowledge generation of RSA parameters. *Lecture Notes in Computer Science*, 1355:89–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cohen:1987:CCI

[Coh87a] Fred Cohen. A cryptographic checksum for integrity protection. *Computers and Security*, 6(6):505–510, December 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900319.

Cohen:1987:IIP

[Coh87b] Fred Cohen. *Introductory Information Protection*. ????, ????, 1987. ISBN ???? ???? pp. LCCN ???? URL http://all.net/books/ip/.

Cohen:1994:SCC

[Coh94] Frederick B. Cohen. *A short course in computer viruses*. Wiley, New York, second edition, 1994. ISBN 0-471-00769-2. xi + 250 pp. LCCN QA76.76.C68 C64 1994. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1027.html.

Cohen:1996:RRA

[Coh96] J. E. Cohen. A right to read anonymously: a closer look at "copyright management" in cyberspace. *Connecticut Law Review*, 28 (??):981–1039, ???? 1996. ISSN 0010-6151. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/063321.html.

Cohen:1999:MNSk

[Coh99] Fred Cohen. Managing network security: The limits of cryptography. *Network Security*, 1999(11):7–11, November 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800800033.

Colaco:1864:CRO

[Col64] F. N. Colaço. *A cryptographia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quaesquer que sejao os caracteres empregados. (Portuguese) [Cryptography revealed, or, the art of translating and deciphering obscure writings, whatever the characters employed]*. De Santos e Cia, Pernambuco, Brazil, 1864. 93 pp. LCCN Z104 .C68 1846.

CPI:1976:CMS

[Com76] Computation Planning Incorporated. Cryptopak: modular subroutine library for cryptographic transformation. Report, Computation Planning Incorporated, Bethesda, MD, USA, 1976.

Cominsky:1987:CAP

[Com87] Isabeth Cominsky. Cryptology: ancient problem modern solutions. Thesis (M.S.), State University of New York, College of

Technology at Utica/Rome, Utica/Rome, NY, USA, 1987. iv + 91 pp.

Comba:1990:ECI

[Com90] P. G. Comba. Exponentiation cryptosystems on the IBM PC. *IBM Systems Journal*, 29(4): 526–538, 1990. CODEN IBMSA7. ISSN 0018-8670.

CSL:1994:DES

[Com94a] Computer Systems Laboratory (U.S.). *Data Encryption Standard (DES)*. Washington, DC, USA, 1994. 18 pp. Category: computer security, subcategory: cryptography. Supersedes FIPS PUB 46-1–1988 January 22. Reaffirmed December 30, 1993. Shipping list no.: 94-0171-P.

CSL:1994:EES

[Com94b] Computer Systems Laboratory (U.S.). *Escrowed Encryption Standard (EES)*. Washington, DC, USA, February 9, 1994. 7 pp. Category: computer security, subcategory: cryptography.

CSL:1994:SRC

[Com94c] Computer Systems Laboratory (U.S.). *Security requirements for cryptographic modules*. National Technical Information Service, Washington, DC, USA, January 11, 1994. 39 pp. Supersedes FIPS PUB 140–1982 April 14. Category: computer security, subcategory: cryptography. Shipping list no.: 94-0172-P.

CERT:1996:PSA

[Com96] Computer Emergency Response Team. *Proceedings of the sixth annual USENIX Security Symposium, focusing on applications of cryptography, July 22–25, 1996, San Jose, California*. USENIX Association, Berkeley, CA, USA, 1996. ISBN 1-880446-79-0. 214 pp. LCCN QA 76.9 A25 U83 1996. Sponsored by the USENIX Association; cosponsored by UniForum in cooperation with the Computer Emergency Response Team (CERT).

CEC:1997:EST

[Com97] Commission of the European Communities. *Ensuring security and trust in electronic communication: towards a European framework for digital signatures and encryption*. COM (97) 503 final COM (Commission of the European Communities); (97) 503 final. Office for Official Publications of the European Communities, Luxembourg, Luxembourg, 1997. ISBN 92-78-25763-X. 35 pp. LCCN ????

Chiba:1999:AGD

[COM99] K. Chiba, H. Ohwada, and

F. Mizoguchi. Acquiring graphic design knowledge with nonmonotonic inductive learning. *Lecture Notes in Computer Science*, 1634:56–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Conradi:1739:CDS

[Con39] David Arnold Conradi. *Cryptographia denudata; sive, Ars deciferandi, quae occulte scripta sunt in quocunque linguarum genere, praecipue in Germanica, Batava, Latina, Anglica, Gallica, Italica, Graeca.* Apud P. Bonk, Lugduni Batavorum, 1739. 73 pp. LCCN Z103 .C66.

Conklin:1998:SCO

[Con98] Edward K. Conklin. Smart cards and the Open Terminal Architecture. *Dr. Dobb's Journal of Software Tools*, 23(12):70, 72, 74, 76, 78, 80, December 1998. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ddj/1998/1998_12/../../../ftp/1998/1998_12/sc_ota.txt`. See errata [Con99a].

Conklin:1999:ESC

[Con99a] Edward K. Conklin. Errata: "Smart Cards and the Open Terminal Architecture" (DDJ, December 1998). *Dr. Dobb's Journal of Software Tools*, 24 (2):18, February 1999. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/1999/9902/9902toc.htm`. See [Con98].

Contini:1999:DPD

[Con99b] Scott Contini. On differential properties of data-dependent rotations and their use in MARS and RC6. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm`; `http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf`; `http://www.nist.gov/aes`. No slides for the conference talk are available.

Coombs:1983:MC

[Coo83] Allen W. M. Coombs. The making of Colossus. *Annals of the History of Computing*, 5(3):253–259, July/September 1983. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1983/pdf/a3253.pdf`; `http://www.computer.org/annals/an1983/a3253abs.htm`.

Coppersmith:1984:FEL

[Cop84] D. Coppersmith. Fast evaluations of logarithms in fields of characteristic two.

IEEE Transactions on Information Theory, IT-30 (4):587–594, ???? 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Coppersmith:1987:C

[Cop87] D. Coppersmith. Cryptography. *IBM Journal of Research and Development*, 31 (2):244–248, March 1987. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Coppersmith:1989:AID

[Cop89] D. Coppersmith. Analysis of ISO/CCITT document X.509 annex D. Internal memo., IBM T. J. Watson Center, Yorktown Heights, NY, USA, June 11, 1989. ?? pp.

Coppersmith:1994:DES

[Cop94a] D. Coppersmith. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, 38(3):243–250, March 1994. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http://www.almaden.ibm.com/journal/rd38-3.html#two`.

Coppersmith:1994:ACS

[Cop94b] Don Coppersmith. Attack on the cryptographic scheme NIKS–TAS. In Desmedt [Des94b], pages 294–307. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390294.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0839/08390294.pdf`.

Charnes:1995:CSE

[COP+95a] C. Charnes, Luke O'Connor, Józef P. Pieprzyk, Reihaneh Safavi-Naini, and Yuliang Zheng. Comments on Soviet encryption algorithm. *Lecture Notes in Computer Science*, 950: 433–438, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500433.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0950/09500433.pdf`.

Coppersmith:1995:ACA

[Cop95b] D. Coppersmith, editor. *Advances in cryptology: 15th Annual international conference — August 1995, Santa Barbara, CA*, number 963 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-60221-6. LCCN QA76.9.A25 C79 1995.

Coppersmith:1995:FSR

[Cop95c] D. Coppersmith. Finding a small root of a univariate modular equation. IBM Research Report RC 20223, IBM T. J. Watson Center, Yorktown Heights, NY, USA, October 11, 1995. Revised November 8, 1995.

Coppersmith:1995:ACC

[Cop95d] Don Coppersmith, editor. *Advances in cryptology, CRYPTO '95: 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27–31, 1995: proceedings*, volume 963 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=963`. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Coppersmith:1998:C

[Cop98] D. Coppersmith. Crypto '95. *Lecture Notes in Computer Science*, 1440: 191–198, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coppersmith:1999:WQS

[Cop99] D. Coppersmith. Weakness in quaternion signatures. In Wiener [Wie99], pages 305–314. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Corcoran:1998:MFS

[Cor98] David Corcoran. Muscle flexes smart cards into Linux. *Linux Journal*, 52: ??, August 1998. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Coron:1999:SRSa

[Cor99] J.-S. Coron. On the security of random sources. *Lecture Notes in Computer Science*, 1560:29–42, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coppersmith:1986:DL

[COS86] Don Coppersmith, Andrew M. Odlyzko, and Richard Schroeppel. Discrete logarithms in GF(p). *Algorithmica*, 1(1):1–15, 1986. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Courville:1986:MCC

[Cou86] Joseph B. Courville. *Manual for cryptanalysis of the columnar double transposition cipher: a study of cryptanalysis*. J. B. Courville, 10240 Virginia Ave, South Gate, CA, 90280, USA, 1986. iv + 91 pp.

Courington:1993:PEA

[Cou93] Jeff Courington. Printer encryption on AIX. *Sys Admin: The Journal for UNIX Systems Administrators*, 2(4):47–??, July/August 1993. CODEN SYADE7. ISSN 1061-2688.

Coutinho:1999:MCN

[Cou99] S. C. Coutinho. *The mathematics of ciphers: number theory and RSA cryptography*. A. K. Peters, Ltd., Wellesley, MA, USA, 1999. ISBN 1-56881-082-2. xv + 196 pp. LCCN QA241 .C69513 1999.

Cremonini:1999:CCA

[COZ99] M. Cremonini, A. Omicini, and F. Zambonelli. Coordination in context: Authentication, authorisation and topology in mobile agent applications. *Lecture Notes in Computer Science*, 1594: 416–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1987:ACE

[CP87] David Chaum and Wyn L. Price, editors. *Advances in Cryptology–EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13–15, 1987: Proceedings*, volume 304 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Chaum:1988:ACE

[CP88] David Chaum and Wyn L. Price, editors. *Advances in cryptology — EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13–15, 1987: proceedings*, volume 304 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E9631 1987; QA267.A1 L43 no.304. Sponsored by the International Association for Crytologic Research.

Camion:1991:KHF

[CP91] P. Camion and J. Patarin. The knapsack hash function proposed at Crypto '89 can be broken. *Lecture Notes in Computer Science*, 547:39–53, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1993:WDO

[CP93] D. Chaum and T. Pryds Pedersen. Wallet databases with observers. *Lecture Notes in Computer Science*, 740:89–105, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chae:1994:AMA

[CP94] Hoon Lim Chae and Joong Lee Pil. Another method for attaining security against adaptively chosen ciphertext attacks. *Lecture Notes in Computer Science*, 773: 420–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chen:1995:NGS

[CP95] L. Chen and T. P. Pedersen. New group signature schemes. *Lecture Notes in Computer Science*, 950: 171–181, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1998:E

[CP98] D. Chaum and W. L. Price. Eurocrypt '87. *Lecture Notes in Computer Science*, 1440:69–74, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chung:1998:DWCa

[CPO+98] Tae-Yun Chung, Kang-Seo Park, Young-Nam Oh, Dong-Ho Shin, and Sang-Hui Park. Digital watermarking for copyright protection of MPEG2 compressed video. In IEEE [IEE98c], pages 336–337. CODEN DTPEEL. ISBN ???? ISSN 0747-668X. LCCN ???? IEEE catalog number 98CH36160.

Charney:1997:PSC

[CPOR97] S. Charney, S. Perrin, S. Orlowski, and N. Reaburn. Panel session: Cryptographic policy guidelines. *Lecture Notes in Computer Science*, 1270:126–??, 1997.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cheon:1998:TEA

[CPPK98] Jung Hee Cheon, S. M. Park, S. W. Park, and D. Kim. Two efficient algorithms for arithmetic of elliptic curves using Frobenius map. *Lecture Notes in Computer Science*, 1431: 195–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Camenisch:1995:BSB

[CPS95] J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler. Blind signatures based on the discrete logarithm problem. *Lecture Notes in Computer Science*, 950:428–432, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chor:1985:KTP

[CR85] Benny Chor and Ronald L. Rivest. A knapsack type public key cryptosystem based on arithmetic in finite fields (preliminary draft). In Blakley and Chaum [BC85], pages 54–65. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=54. See also revised version in [CR88c].

Carroll:1988:ACP

[CR88a] John M. Carroll and Lynda Robbins. The automated cryptananysis of polyalphabetic ciphers. *Computers and Security*, 7(1):104, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888905354.

Carroll:1988:CC

[CR88b] John M. Carroll and Lynda E. Robbins. Computer cryptanalysis. Report 223, Department of Computer Science, University of Western Ontario, London, UK, 1988. ISBN 0-7714-1070-0. 55 pp.

Chor:1988:KTP

[CR88c] Benny Chor and Ronald L. Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, IT-34(5, part 1):901–909, 1988. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Chaum:1991:USD

[CR91] David Chaum and Sandra Roijakkers. Unconditionally secure digital signatures. *Lecture Notes in Computer Science*, 537: 206–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370206.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370206.pdf.

Caronni:1997:HEE

[CR97] Germano Caronni and Matt Robshaw. How exhausting is exhaustive search? *CryptoBytes*, 2(3):1, 3–6, Winter 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n3.pdf.

Crawford:1992:ASA

[Cra92] David J. Crawford. Autoscritcher and the superscritcher: Aids to cryptanalysis of the German Enigma cipher machine, 1944–1946. *Annals of the History of Computing*, 14 (3):9–22, July/September 1992. CODEN AHCOE5. ISSN 0164-1239.

Craig:1996:CDC

[Cra96] Richard Craig. Considerations of data compression and symmetric encryption techniques for a personal communications service. Thesis (M.S.), University of Mississippi, Oxford, MS, USA, 1996. various pp.

Craver:1997:PSP

[Cra97] Scott Craver. On public-key steganography in the presence of an active warden. Research report RC 20931 (92684), IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, July 23, 1997. 17 pp.

Craver:1998:PKS

[Cra98] Scott Craver. On public-key steganography in the presence of an active warden. *Lecture Notes in Computer Science*, 1525: 355–368, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250355.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250355.pdf.

Cramer:1999:ISC

[Cra99] R. Cramer. Introduction to secure computation. *Lecture Notes in Computer Science*, 1561:16–62, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Crepeau:1990:VDS

[Cré90] Claude Crépeau. Verifiable disclose for secrets and applications (abstract). *Lecture Notes in Computer Science*, 434:150–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340150.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0434/04340150.pdf`.

Crepeau:1997:ECP

[Cre97] C. Crepeau. Efficient cryptographic protocols based on noisy channels. *Lecture Notes in Computer Science*, 1233:306–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Contini:1999:IAS

[CRRY99] S. Contini, R. L. Rivest, M. J. B. Robshaw, and Y. L. Yin. Improved analysis of some simplified variants of RC6. In Knudsen [Knu99c], pages 1–15. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Chaum:1983:ACP

[CRS83] David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors. *Advances in Cryptology: proceedings of CRYPTO 82*. Plenum Press, New York, NY, USA; London, UK, 1983. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982.

Chaum:1998:Ca

[CRS98] D. Chaum, R. L. Rivest, and A. T. Sherman. Crypto '82. *Lecture Notes in Computer Science*, 1440:13–20, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Crypto:1981:ACP

[CRY81] *Advances in cryptology: proceedings of CRYPTO*, page various, 1981. Plenum Press, New York, NY, USA; London, UK. Volumes for 1984 to 1989 were published in the Springer-Verlag Lecture Notes in Computer Science series.

CryptoBytes:1995:C

[Cry95] *CryptoBytes*, 1995. URL `http://www.rsa.com/rsalabs/pubs/cryptobytes/html/article_index.html`; `http://www.rsa.com/rsalabs/pubs/cryptobytes/html/subscribe.html`; `http://www.rsa.com/rsalabs/pubs/cryptobytes/index.html`; `mailto:bytes-ed@rsa.com`. RSA Data Security, Inc., RSA Laboratories West, 2955 Campus Drive, Suite 400, San Mateo, CA 94403-1031, USA; RSA Laboratories East, 20

Crosby Drive, Bedford, MA 01730-1402, USA. CryptoBytes is the technical newsletter on cryptography from RSA Laboratories, a division of RSA Data Security, Inc. It is a free publication, and all issues are available on the World Wide Web.

Cesarini:1983:ACC

[CS83] F. Cesarini and G. Soda. An algorithm to construct a compact *B*-tree in case of ordered keys. *Information Processing Letters*, 17 (1):13–16, July 19, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chepyzhov:1991:FCA

[CS91] V. Chepyzhov and B. Smeets. On a fast correlation attack on certain stream ciphers. *Lecture Notes in Computer Science*, 547:176–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chabaud:1996:CSS

[CS96a] F. Chabaud and J. Stern. The cryptographic security of the syndrome decoding problem for rank distance codes. *Lecture Notes in Computer Science*, 1163: 368–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chambers:1996:RLM

[CS96b] W. G. Chambers and S. J. Shepherd. Register locking in mutual clock control cipher keystream generators. In Gollmann [Gol96d], page ?? CODEN LNCSD9. ISBN 3-540-60865-6 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F38 1996. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1039.htm`; `http://www.springerlink.com/content/978-3-540-60865-3`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1039`.

Cusick:1996:BNFb

[CS96c] Thomas W. Cusick and Pantelimon Stănică. Bounds on the number of functions satisfying the Strict Avalanche Criterion. *Information Processing Letters*, 60(4):215–219, November 25, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [YT96].

Camenisch:1997:EGS

[CS97a] J. Camenisch and M. Stadler. Efficient group signature schemes for large groups. *Lecture Notes in Computer Science*, 1294:410–??, 1997. CODEN LNCSD9. ISSN

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

Chambers:1997:RLM

[CS97b] W. G. Chambers and S. J. Shepherd. Register locking in mutual clock control cipher keystream generators. *Electronics Letters*, 33(12): 1020–1021, June 5, 1997. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic).

Chen:1997:NIC

[CS97c] Jonathan J-R Chen and Ping-Tai Sun. New ID-based cryptosystem based on number theory. *International Journal of Computer Systems Science and Engineering*, 12(1):37–41, January 1997. CODEN CSSEEI. ISSN 0267-6192.

Coppersmith:1997:PAP

[CS97d] Don Coppersmith and Igor E. Shparlinski. On polynomial approximation and the parallel complexity of the discrete logarithm and breaking the Diffie–Hellman cryptosystem. Research report RC 20724 (91825), IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, February 3, 1997. vi + 103 pp.

Canteaut:1998:COM

[CS98a] Anne Canteaut and Nicolas Sendrier. Cryptanalysis of the original McEliece cryptosystem. *Lecture Notes in Computer Science*, 1514: 187–199, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cramer:1998:PPK

[CS98b] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. *Lecture Notes in Computer Science*, 1462:13–25, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620013.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620013.pdf`.

Coradeschi:1999:ASV

[CS99] S. Coradeschi and A. Saffiotti. Anchoring symbols to vision data by fuzzy logic. *Lecture Notes in Computer Science*, 1638:104–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1989:SCF

[CSB89] David Chaum and Ingrid Schaumuller-Bichl, editors. *Smart card 2000: the future of IC cards: proceedings of the IFIP WG 11.6 International Conference on Smart Card 2000–the Future of IC*

Cards, Laxenburg, Austria, 19–20 October 1987. North-Holland, Amsterdam, The Netherlands, 1989. ISBN 0-444-70545-7. LCCN TK7895.S62 I35 1987.

Csirmaz:1995:SSM

[Csi95] L. Csirmaz. The size of a share must be large. *Lecture Notes in Computer Science*, 950:13–22, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coppersmith:1994:ABP

[CSV94] Don Coppersmith, Jacques Stern, and Serge Vaudenay. Attacks on the birational permutation signature schemes. *Lecture Notes in Computer Science*, 773:435–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chang:1997:GSS

[CT97] Chin-Chen Chang and Hui-Min Tsai. A generalized secret sharing scheme. *The Journal of Systems and Software*, 36(3):267–??, ???? 1997. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Chen:1999:TPS

[CT99a] Z.-G. Chen and S. E. Tavares. Toward provable security of substitution-permutation encryption networks. *Lecture Notes in Computer Science*, 1556: 43–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Collberg:1999:SWM

[CT99b] Christian Collberg and Clark Thomborson. Software watermarking: models and dynamic embeddings. In ACM [ACM99a], pages 311–324. ISBN 1-58113-095-3. LCCN ???? URL `http://www.acm.org:80/pubs/citations/proceedings/plan/292540/p311-collberg/`.

Cox:19xx:NST

[CTSxx] B. Cox, J. D. Tygar, and M. Sirbu. NetBill security and transaction protocol. ????, 19xx. URL `http://www.ini.cmu.edu/netbill/home.html`.

Chao:1994:DEC

[CTT94] Jinhui Chao, Kazuo Tanada, and Shigeo Tsujii. Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks. In Desmedt [Des94b], pages 50–55. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994.

URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390050.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390050.pdf.

Currier:1998:MPT

[Cur98] Prescott Currier. My "Purple" trip to England in 1941. In Deavours et al. [DKK+98], pages 287–295. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Cusick:1995:CPK

[Cus95] Thomas W. Cusick. Cryptanalysis of a public key system based on Diophantine equations. *Information Processing Letters*, 56(2): 73–75, October 27, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Cusick:1996:BNFa

[Cus96] Thomas W. Cusick. Bounds on the number of functions satisfying the Strict Avalanche Criterion. *Information Processing Letters*, 57(5):261–263, March 11, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See comment [YT96].

Cusick:1997:CRN

[Cus97] Thomas W. Cusick. A comparison of RSA and the Naccache-Stern public-key cryptosystem. *Lecture Notes in Computer Science*, 1189:111–116, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ciminiera:1989:AMM

[CV89] L. Ciminiera and A. Valenzano. Authentication mechanisms in microprocessor-based local area networks. *IEEE Transactions on Software Engineering*, 15(5): 654–658, May 1989. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=24716.

Calvelli:1993:ARS

[CV93] Claudio Calvelli and Vijay Varadharajan. Authentication and revocation in SPM extended abstract. *Operating Systems Review*, 27(4): 42–57, October 1993. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Chabaud:1995:LBD

[CV95] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. *Lecture Notes in Computer Science*, 950: 356–365, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cohn:1999:MC

[CV99] A. G. Cohn and A. C. Varzi. Modes of connection. *Lecture Notes in Computer Science*, 1661:299–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chaum:1991:CSU

[CvHP91] David Chaum, Eugène van Heijst, and Birgit Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer (extended abstract). *Lecture Notes in Computer Science*, 576:470–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760470.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760470.pdf`.

Chang:1991:BCC

[CW91a] Chin-Chen Chang and Tzong-Chen Wu. Broadcasting cryptosystem in computer networks using interpolating polynomials. *Computer Systems Science and Engineering*, 6(3):185–??, July 1991. CODEN CSSEEI. ISSN 0267-6192.

Cusick:1991:RIC

[CW91b] Thomas W. Cusick and Michael C. Wood. The REDOC II cryptosystem. *Lecture Notes in Computer Science*, 537:545–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370545.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370545.pdf`.

Campbell:1993:G

[CW93] K. W. Campbell and M. J. Wiener. DES is not a group. *Lecture Notes in Computer Science*, 740:512–520, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chmora:1994:ECC

[CW94] Andrew Chmora and Stephen B. Wicker, editors. *Error control, cryptology, and speech compression: Workshop on Information Protection, Moscow, Russia, December 6–9, 1993: Selected Papers*, volume 829 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 3-540-58265-7 (Berlin), 0-387-58265-7 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 W668 1993. DM39.00. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0829.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=829.

Chang:1997:SCO

[CW97] Chin-Chen Chang and Tzong-Chen Wu. A smart card oriented password authentication scheme based on Rabin's public key cryptosystem. *Internat. J. Inform. Management Sci.*, 8 (3):63–73, 1997. CODEN IIMSEQ. ISSN 1017-1819.

Ceruzzi:1991:RGC

[CWM+91] Paul Ceruzzi, Eric A. Weiss, John Walker Mauer, Thomas Drucker, Peggy Aldrich Kidwell, and K. W. Smillie. Reviews: Grosch: Computer: Bit slices from a life; Tomayko: Computers in spaceflight: The NASA Experience; Bülow: Denk, Maschine! Geschichten über Robotor, computer und Kunstliche Inteligenz; Napier: Rabdology; Charlesworth: Calculators & Computers; Calculators & Computers — The 20th Century; Transistors. forty years of computing, Datamation; Bennett: The industrial instrument — Master of industry, servant of management: Automatic control in the process industries, 1900–1940. Kapera: The Enigma Bulletin. *Annals of the History of Computing*, 13(4):364–368, October/December 1991. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1991/pdf/a4364.pdf; http://www.computer.org/annals/an1991/a4364abs.htm.

Coppersmith:1998:CT

[CWSK98] Don Coppersmith, David Wagner, Bruce Schneier, and John Kelsey. Cryptanalysis of TWOPRIME. *Lecture Notes in Computer Science*, 1372:32–48, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.counterpane.com/twoprime.html.

Chang:1998:BSC

[CWY98] Chin-Chen Chang, Tzong-Chen Wu, and Yi-Shiung Yeh. Broadcasting secrets in communication networks. *International Journal of Computer Systems Science and Engineering*, 13

(2):121–124, March 1998. CODEN CSSEEI. ISSN 0267-6192.

Craver:1998:TTL

[CYY98] S. Craver, B. L. Yeo, and M. Yeung. Technical trials and legal tribulations. *Communications of the Association for Computing Machinery*, 41(7):45–54, July 1998. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073119.html.

Cao:1990:DKC

[CZ90] Zhen Fu Cao and Bao Dong Zheng. A discussion on knapsack cryptosystems concealed by a matrix cover. *J. Harbin Inst. Tech.*, 6:34–41, 1990. ISSN 0367-6234.

DeMillo:1983:ACC

[D+83] Richard A. DeMillo et al. *Applied cryptology, cryptographic protocols, and computer security models*, volume 29 of *Proceedings of symposia in applied mathematics. AMS short course lecture notes.* American Mathematical Society, Providence, RI, USA, 1983. ISBN 0-8218-0041-8. ISSN 0160-7634. xi + 192 pp. LCCN QA1 .A56 v.29 1981. Expanded version of notes prepared for the AMS short course entitled Cryptology in revolution, mathematics and models, held in San Francisco, CA, Jan. 5–6, 1981, by Richard A. DeMillo and others.

Dittmann:1998:MSW

[D+98] Jana Dittmann et al., editors. *Multimedia and security: workshop at ACM Multimedia '98, Bristol, United Kingdom, September 12–13, 1998*, volume 41 of *GMD Report*. ACM Press, New York, NY 10036, USA, 1998. ISBN ???? LCCN ????

DAgapeyeff:1939:CC

[D'A39] Alexander D'Agapeyeff. *Codes and ciphers.* Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1939. 160 pp. LCCN Z104 .D3 1939.

DAgapeyeff:1971:CC

[D'A71] Alexander D'Agapeyeff. *Codes and ciphers.* Gryphon Books, Ann Arbor, MI, USA, 1971. ISBN ???? 160 pp. LCCN Z103 .D35 1971. Reprint of [D'A39].

Daemen:1995:HFC

[Dae95] Joan Daemen. *Hash Function and Cipher Design: Strategies Based on Linear and Differential Cryptanalysis.* Ph.D. thesis, Katholieke Universiteit Leuven, Leuven, Belgium, March 1995. 280 pp. URL http://wwwlib.umi.com/dissertations/fullcit/f548867.

Daemen:1998:MSK

[Dae98] J. Daemen. Management of secret keys: Dynamic key handling. *Lecture Notes in Computer Science*, 1528: 264–276, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Daemen:1999:RAI

[Dae99] Joan Daemen. Resistance against implementation attacks: a comparative study of the AES proposals. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Dalton:1997:KSW

[Dal97] Curt Dalton. *Keeping the secret: the Waves and NCR: Dayton, Ohio 1943–1946*. C. Dalton, Dayton, OH, USA, 1997. ISBN 1-4922-0896-5. 72 pp. LCCN ????

Damgaard:1990:ACE

[Dam90a] I. B. Damgård, editor. *Advances in Cryptology–EUROCRYPT '90: Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 21–24, 1990: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). LCCN QA76.9.A25 E964 1990. DM69.00.

Damgaard:1990:DPH

[Dam90b] I. B. Damgård. A design principle for hash functions. In Brassard [Bra90c], pages 416–427. CODEN LNCSD9. ISBN 0-387-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Damgaard:1991:ACE

[Dam91a] I. B. Damgård, editor. *Advances in cryptology — EUROCRYPT '90: Workshop on the Theory and Ap-*

plication of Cryptographic Techniques, Aarhus, Denmark, May 21–24, 1990: proceedings, volume 473 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. CODEN LNCSD9. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1990. DM69.00.

Damgaard:1991:TPP

[Dam91b] Ivan Bjerre Damgård. Towards practical public key systems secure against chosen ciphertext attacks. *Lecture Notes in Computer Science*, 576:445–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760445.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760445.pdf`.

Damgard:1994:PPS

[Dam94a] I. B. Damgard. Practical and provably secure release of a secret and exchange of signatures. *Lecture Notes in Computer Science*, 765:200–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Damgaard:1994:PPS

[Dam94b] Ivan Bjerre Damgård. Practical and provably secure release of a secret and exchange of signatures. *Lecture Notes in Computer Science*, 765:200–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650200.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650200.pdf`.

Dam:1996:RPG

[Dam96] Kenneth W. Dam. *The role of private groups in public policy: cryptography and the National Research Council*. Occasional papers from the Law School, the University of Chicago; no. 38. Law School, The University of Chicago, Chicago, IL, USA, 1996. 29 pp. LCCN QA76.9.A25 D34 1996.

Damgard:1998:E

[Dam98] I. B. Damgard. Eurocrypt '90. *Lecture Notes in Computer Science*, 1440: 111–118, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Damgaard:1999:CSZ

[Dam99a] I. Damgaard. Commitment schemes and zero-knowledge protocols. *Lecture Notes in Computer Science*, 1561:63–86, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Damgaard:1999:LDS

[Dam99b] I. B. (Ivan Bjerre) Damgård, editor. *Lectures on data security: modern cryptology in theory and practice*, volume 1561 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-65757-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25L46 1999.

Danisch:1995:RES

[Dan95] H. Danisch. RFC 1824: The Exponential Security System TESS: An identity-based cryptographic protocol for authenticated key-exchange (E.I.S.S.-Report 1995/4), August 1995. URL `ftp://ftp.internic.net/rfc/rfc1824.txt`; `https://www.math.utah.edu/pub/rfc/rfc1824.txt`. Status: INFORMATIONAL.

Danthine:1996:ECM

[Dan96] A. Danthine, editor. *European Conference on Multimedia Applications and Technologies (ECMAST '96): Louvain-La-Neuve, May 28–30, 1996*. AEI, Milano, Italy, 1996. LCCN ????

Dang:1997:AAC

[Dan97] Zhe Dang. Automated analysis of cryptographic protocols using the ASTRAL model checker. Thesis (M.S.), University of California, Santa Barbara, Santa Barbara, CA, USA, 1997.

Darnell:1997:CCI

[Dar97] Mike Darnell, editor. *Cryptography and coding: 6th IMA conference, Cirencester, UK, December 17–19, 1997: proceedings*, volume 1355 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-63927-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C76 1997. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1355.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1355`.

DRC:1985:AAN

[Dat85] Datapro Research Corporation. *All about network ac-*

cess control and data encryption devices: with in-depth analyses of leading devices. Datapro Research Corporation, Delran, NJ, USA, June 1985. 65 pp.

Davida:1979:IHS

[Dav79] G. I. Davida. III. 'Hellman's scheme breaks DES in its basic form'. *IEEE Spectrum*, 16(7):39, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Davida:1981:CAR

[Dav81] George I. Davida. The case against restraints on non-governmental research in cryptography. *Communications of the Association for Computing Machinery*, 24(7):445–450, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). This is an opposing view published with [Ame81].

Davies:1985:MAA

[Dav85] Donald Watts Davies. A message authenticator algorithm suitable for a mainframe computer. In Blakley and Chaum [BC85], pages 393–400. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=393`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Davies:1991:ACE

[Dav91] Donald Watts Davies, editor. *Advances in cryptology — EUROCRYPT '91: Workshop on the Theory and Application of Cryptography Techniques, Brighton, UK, April 8–11, 1991: proceedings*, volume 547 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. CODEN LNCSD9. ISBN 0-387-54620-0 (New York), 3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991. Rev. and expanded papers from the meeting which was sponsored by the International Association for Cryptology Research (IACR) and others.

Davis:1994:RAC

[Dav94] Donald T. Davis. Review: Applied Cryptography. *;lo-*

gin: the USENIX Association newsletter, 19(2):46–??, March/April 1994. CODEN LOGNEM. ISSN 1044-6397.

Davis:1995:KPR

[Dav95] Don Davis. Kerberos plus RSA for world wide Web security. In USENIX Association [USE95c], pages 185–188. ISBN 1-880446-74-X. LCCN HF5548.33. U84 1995(1). URL `http://www.usenix.org/publications/library/proceedings/ec95/davis.html`.

Davis:1996:CDP

[Dav96] Don Davis. Compliance defects in public key cryptography. In USENIX Association [USE96g], pages 171–178. URL `http://www.usenix.org/publications/library/proceedings/sec96/davis.html`.

David:1998:WWI

[Dav98a] Charles David. A World War II German army field cipher and how we broke it. In Deavours et al. [DKK+98], pages 339–360. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Davies:1998:E

[Dav98b] D. W. Davies. Eurocrypt '91. *Lecture Notes in Computer Science*, 1440: 127–134, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Davies:1998:NIH

[Dav98c] D. W. Davies. New information on the history of the Siemens and Halske T52 cipher machines. In Deavours et al. [DKK+98], pages 455–460. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Davies:1998:LCM

[Dav98d] Donald W. Davies. The Lorenz cipher machine SZ42. In Deavours et al. [DKK+98], pages 517–539. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Dawson:1985:COL

[Daw85] M. J. Dawson. *Cryptanalysis of ornithological literature*, volume 4 of *Caliologists' series*. Oriel Stringer, Brighton, 1985. ISBN 0-948122-04-8 (paperback). 40 pp. LCCN ????

Dawson:1993:CSG

[Daw93] E. Dawson. Cryptanalysis of summation generator. *Lecture Notes in Computer Science*, 718:209–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dawson:1996:CSR

[Daw96] Donald A. Dawson. *Cryptanalysis of the single rotor cipher machine*, volume 73 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1996. ISBN 0-89412-262-2. iv + 213 pp. LCCN ????

Denning:1981:SRR

[DB81] Peter J. Denning and David H. Brandin. Special report: Report of the Public Cryptography Study Group. *Communications of the Association for Computing Machinery*, 24(7): 434, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

denBoer:1988:CF

[dB88] Bert den Boer. Cryptanalysis of F.E.A.L. *Lecture Notes in Computer Science*, 330:293–299, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Denning:1989:EET

[DB89] Dorothy Elizabeth Robling Denning and William E. Baugh, Jr. *Encryption and evolving technologies: tools of organized crime and terrorism*. US Working Group on Organized Crime monograph series. National Strategy Information Center, Washington, DC, USA, 1989. ISSN 1093-7269. ii + 52 pp.

denBoer:1991:ALT

[dB91] B. den Boer and A. Bosselaers. An attack on the last two rounds of MD4. In Feigenbaum [Fei91], pages 194–203. CODEN LNCSD9. ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1991. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0576.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=576`. Conference held Aug. 11–15, 1991, at the University of California, Santa Barbara.

denBoer:1994:CCF

[dB94] B. den Boer and A. Bosselaers. Collisions for the compression function of MD5. In Stinson [Sti94], pages 293–304. CODEN

LNCSD9. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1993. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0773.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=773.

Denning:1996:TKE

[DB96] Dorothy E. Denning and Dennis K. Branstad. A taxonomy for key escrow encryption systems. *Communications of the Association for Computing Machinery*, 39(3):34–40, March 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/227239.html; http://www.acm.org/pubs/toc/Abstracts/cacm/227239.html.

Daswani:1999:EEC

[DB99] N. Daswani and D. Boneh. Experimenting with electronic commerce on the PalmPilot. In Franklin [Fra99], pages 1–16. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Boer:1991:ALT

[dBB91] Bert den Boer and Antoon Bosselaers. An attack on the last two rounds of MD4. *Lecture Notes in Computer Science*, 576: 194–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760194.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760194.pdf.

Daemen:1993:CSH

[DBGV93] Joan Daemen, Antoon Bosselaers, Rene Govaerts, and Joos Vandewalle. Collisions for Schnorr's hash function FFT-Hash presented at Crypto'91. *Lecture Notes in Computer Science*, 739:477–480, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dobbertin:1996:RSV

[DBP96] H. Dobbertin, A. Bosselaers, and B. Preneel. RIPEMD-160: a strengthened version of RIPEMD. In Gollmann [Gol96d], pages 71–82. CODEN LNCSD9. ISBN 3-540-60865-6 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F38 1996. URL http://www.esat.kuleuven.ac.be/~bosselae/ripemd160. (An updated and corrected version is available at ftp.esat.kuleuven.ac.be, directory /pub/COSIC/bosselae/ripemd/.).

DHalluin:1999:ASR

[DBR+99] C. D'Halluin, G. Bijnens, V. Rijmen, Preneel, and B. Attack on six rounds of CRYPTON. In Knudsen [Knu99c], pages 46–59. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

DeWin:1996:FSI

[DBVD96] E. De Win, A. Bosselaers, S. Vandenberghe, and P. De Getsem. A fast software implementation for arithmetic operations in GF(20n). *Lecture Notes in Computer Science*, 1163:65–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

deJonge:1986:ASR

[dC86] W. de Jonge and D. Chaum. Attacks on some RSA signatures. In Williams [Wil86b], pages 18–27. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm`; `http://www.springerlink.com/content/978-0-387-16463-2`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=218`.

deJonge:1987:SVR

[dC87] Wiebren de Jonge and David Chaum. Some variations on RSA signatures & their security. In Odlyzko [Odl87b], pages 49–59. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263`. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Daemen:1998:PCF

[DC98a] Joan Daemen and Craig Clapp. The Panama cryptographic function. *Dr. Dobb's Journal of Software Tools*, 23(12):42, 44, 46, 48–49, December 1998. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ddj/1998/1998_12/../../../ftp/1998/1998_12/panama.zip`.

Daemen:1998:FHS

[DC98b] Joan Daemen and Craig S. K. Clapp. Fast hashing and stream encryption with Panama. *Lecture Notes in Computer Science*, 1372:60–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720060.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1372/13720060.pdf`.

DeOca:1998:DRD

[DC98c] C. M. De Oca and D. L. Carver. Design recovery with data mining techniques. *Lecture Notes in Computer Science*, 1394:405–406, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DAmiano:1995:MDM

[DD95] S. D'Amiano and G. Di Crescenzo. Methodology for digital money based on general cryptographic tools. *Lecture Notes in Computer Science*, 950:156–170, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSchutter:1999:ELC

[DD99] B. De Schutter and B. De Moor. The extended linear complementarity problem and the modeling and analysis of hybrid systems. *Lecture Notes in Computer Science*, 1567:70–85, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1995:MNA

[DDB95a] Y. Desmedt, G. Di Crescenzo, and M. Burmester. Multiplicative non-Abelian sharing schemes and their application to threshold cryptography. *Lecture Notes in Computer Science*, 917:21–32, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1995:MNS

[DDB95b] Y. Desmedt, G. Di Crescenzo, and M. Burmester. Multiplicative non-Abelian sharing schemes and their application to threshold cryptography. In Pieprzyk and Safavi-Naini [PSN95a], pages 21–32.

DeSantis:1994:HSF

[DDFY94] A. De Santis, Y. Desmedt, Y. Frankel, and M. Yung. How to share a function securely. In ACM [ACM94c], pages 522–533. ISBN 0-89791-663-8. LCCN QA76 .A15 1994. ACM order no. 508930.

Davio:1985:EHS

[DDG+85] Marc Davio, Yvo Desmedt, Jo Goubert, Frank Hoornaert, and Jean-Jacques Quisquater. Efficient hardware and software implementations for the DES. In Blakley and Chaum [BC85], pages 144–146. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=144. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Delaigle:1997:LCW

[DDGM97] J. F. Delaigle, C. De Vleeschouwer, F. Goffin, and B. Macq. Low cost watermarking based on a human visual model. *Lecture Notes in Computer Science*, 1242:153–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DDJStaff:1998:NVS

[DDJ98a] DDJ Staff. News and views: a Standard Linux? cryptography contest; drives get smaller and Smaller; Perl conference; really embedded systems; programmer shortage?; Beowulf: Linux clustering; Java SPEC released. *Dr. Dobb's Journal of Software Tools*, 23(11): 16, November 1998. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

DDJStaff:1998:NVb

[DDJ98b] DDJ Staff. News and views: Computing olympiad; the public's right to know; smart cards; more Y2K; why Rome burns; biocomputing; new infrared standards; national medals awarded. *Dr. Dobb's Journal of Software Tools*, 23(3): 18, March 1998. CODEN DDJOEB. ISSN 1044-789X.

DDJStaff:1998:NVG

[DDJ98c] DDJ Staff. News and views: Going west; end of an era; electronic messaging available; putting your money where your mouth is; Amiga redux; unscrambling encryption; ergonomic research; PPTP bug. *Dr. Dobb's Journal of Software Tools*, 23(8): 16, August 1998. CODEN DDJOEB. ISSN 1044-789X.

DDJStaff:1998:NVY

[DDJ98d] DDJ Staff. News and views: In your face; who invented the microprocessor?; mixed media; but where will they go for spring break?; quantum computing lives; E-commerce continues to grow...; ...but will smart cards play a role? *Dr. Dobb's Journal of Software Tools*, 23(12): 18, December 1998. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.microcomputerhistory.com/`.

DDJ:1998:NVN

[DDJ98e] DDJ Staff. News and views: New trends in vaporware; distance ed might pay off; life in the fast lane; making friends in Washington; news on OpenGL 1.2; no discounts for schools; let's do lunch; encryption export challenge?; Java fissures; searching for talent in science; nanomedicine. *Dr. Dobb's Journal of Software Tools*, 23(6):18, June 1998. CODEN DDJOEB. ISSN 1044-789X.

DDJStaff:1998:NVN

[DDJ98f] DDJ Staff. News and views: New trends in vaporware; distance ed might pay off; life in the fast lane; making friends in Washington; news on OpenGL 1.2; no discounts for schools; let's do lunch; encryption export challenge?; Java fissures; searching for talent in science; nanomedicine. *Dr. Dobb's Journal of Software Tools*, 23(6):18, June 1998. CODEN DDJOEB. ISSN 1044-789X.

DDJStaff:1998:NVc

[DDJ98g] DDJ Staff. News and views: The secret story of nonsecret encryption; Netscape news; key escrow woes; fingerprint IC. *Dr. Dobb's Journal of Software Tools*, 23(4):18, April 1998. CODEN DDJOEB. ISSN 1044-789X. Discusses a claim by the British GHCQ agency to have invented public-key cryptography in unpublished classified work prior to the RSA and Diffie–Hellman publications.

DDJStaff:1998:NVd

[DDJ98h] DDJ Staff. News and views: The secret story of nonsecret encryption; Netscape news; key escrow woes; fingerprint IC. *Dr. Dobb's Journal of Software Tools*, 23(4):18, April 1998. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/`. Discusses a claim by the British GHCQ agency to have invented public-key cryptography in unpublished classified work prior to the RSA and Diffie–Hellman publications.

DDJstaff:1999:NVR

[DDJ99] DDJ staff. News and views: Real-time Java working group; simulated safety; A house of smart cards; father of ubiquitous computing passes away; electrochemical fabrication. *Dr.*

Dobb's Journal of Software Tools, 24(7):18, July 1999. CODEN DDJOEB. ISSN 1044-789X.

DePaoli:1998:WBS

[DDK98] F. De Paoli, A. L. Dos Santos, and R. A. Kemmerer. Web browsers and security. *Lecture Notes in Computer Science*, 1419:235–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Denny:1994:FR

[DDLM94] T. Denny, Bruce Dodson, Arjen K. Lenstra, and Mark S. Manasse. On the factorization of RSA-120. *Lecture Notes in Computer Science*, 773: 166–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730166.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730166.pdf`.

Delaigle:1996:DW

[DDM96] Jean-François Delaigle, Christophe De Vleeschouwer, and Benoit M. Macq. Digital watermarking. In van Renesse [van96], pages 99–110. CODEN PSISDG. ISBN 0-8194-2033-6. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TS510.S63 v.2659.

Delaigle:1998:PAD

[DDM98] J.-F. Delaigle, C. De Vleeschouwer, and B. Macq. Psychovisual approach to digital picture watermarking. *Journal of Electronic Imaging*, 7(3):628–640, July 1998. CODEN JEIME5. ISSN 1017-9909 (print), 1560-229X (electronic).

Dolev:1991:NC

[DDN91a] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. In ACM [ACM91], pages 542–552. ISBN 0-89791-397-3. LCCN QA 76.6 A13 1991. Full version available from authors.

Dolev:1991:NMC

[DDN91b] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In ACM [ACM91], pages 542–552. ISBN 0-89791-397-3. LCCN QA 76.6 A13 1991. URL `http://www.acm.org/pubs/articles/proceedings/stoc/103418/p542-dolev/p542-dolev.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/103418/p542-dolev/`. IEEE Computer Society order no. 2190.

Darmstaedter:1998:BBW

[DDNM98] V. Darmstaedter, J.-F. Delaigle, D. Nicholson, and B. Macq. A block based watermarking technique for MPEG2 signals: Optimization and validation on real digital TV distribution links. *Lecture Notes in Computer Science*, 1425: 190–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Delsarte:1985:FCM

[DDOP85] P. Delsarte, Y. Desmedt, A. Odlyzko, and P. Piret. Fast cryptanalysis of the Matsumoto–Imai public key scheme. In Beth et al. [BCI85], pages 142–149. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL `http://www.research.att.com/~amo/doc/arch/break.mi.scheme.pdf`; `http://www.research.att.com/~amo/doc/arch/break.mi.scheme.ps`; `http://www.research.att.com/~amo/doc/arch/break.mi.scheme.troff`. Held at the University of Paris, Sorbonne.

Davida:1990:KDS

[DDP90] George I. Davida, Yvo Desmedt, and René Peralta. A key distribution system based on any one-way function (extended abstract). *Lecture Notes in Computer Science*, 434: 75–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340075.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0434/04340075.pdf`.

DeSantis:1994:SSP

[DDP94a] Alfredo De Santis, Giovanni Di Crescenzo, and Giuseppe Persiano. Secret sharing and perfect zero-knowledge. *Lecture Notes in Computer Science*, 773:73–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730073.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0773/07730073.pdf`.

DeSantis:1994:KCQ

[DDP94b] Alfredo De Santis, Giovanni Di Crescenzo, and Guiseppe Persiano. The knowledge complexity of quadratic residuosity languages. *Theoretical Computer Science*, 132(1–2):291–317, September 26, 1994. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-`

bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1994&volume=132&issue=1-2&aid=1595.

DeSantis:1999:NIZ

[DDP99] A. De Santis, G. Di Crescenzo, and G. Persiano. Non-interactive zero-knowledge: a low-randomness characterization of NP (extended abstract). *Lecture Notes in Computer Science*, 1644: 271–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Darmstaedter:1998:LCS

[DDQM98] V. Darmstaedter, J.-F. Delaigle, J. J. Quisquater, and B. Macq. Low cost spatial watermarking. *Computers and Graphics*, 22(4):417–424, August 1, 1998. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.elsevier.com/cas/tree/store/cag/sub/1998/22/4/565.pdf.

deVries:1953:SMC

[de 53] M. de Vries. *Statistical methods in cryptanalysis*. Rapport ZW 1953-014. Math. Centrum Amsterdam, Amsterdam, The Netherlands, 1953. 15 pp.

DeAlvare:1990:HCC

[De 90] Ana Maria De Alvare. How crackers crack passwords. In USENIX Association [USE90], pages 103–112. LCCN QA 76.9 A25 U55 1990.

DeDecker:1993:USK

[De 93a] B. De Decker. Unix security and Kerberos. *Lecture Notes in Computer Science*, 741:257–274, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSchutter:1993:TFA

[De 93b] B. De Schutter. Trends in the fight against computer-related delinquency. *Lecture Notes in Computer Science*, 741:3–19, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSoete:1993:PKC

[De 93c] M. De Soete. Public key cryptography. *Lecture Notes in Computer Science*, 741:33–49, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSantis:1995:ACE

[De 95] Alfredo De Santis, editor. *Advances in cryptology — EUROCRYPT '94: Workshop on the Theory and Application of Cryptographic*

Techniques, Perugia, Italy, May 9–12, 1994: proceedings, volume 950 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-60176-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E965 1995.

DeDecker:1998:ICS

[De 98a] B. De Decker. Introduction computer security. *Lecture Notes in Computer Science*, 1528:377–394, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSantis:1998:E

[De 98b] A. De Santis. Eurocrypt '94. *Lecture Notes in Computer Science*, 1440: 165–172, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSchutter:1998:TFA

[De 98c] B. De Schutter. Trends in the fight against computer-related delinquency. *Lecture Notes in Computer Science*, 1528:1–17, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSmit:1998:GAE

[De 98d] B. De Smit. Generating arithmetically equivalent number fields with elliptic curves. *Lecture Notes in Computer Science*, 1423: 392–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeMoliner:1999:STB

[De 99] Richard De Moliner. *On the Statistical Testing of Block Ciphers*. Ph.D. thesis, Signal and Information Processing Laboratory, Swiss Federal Institute of Technology at Zürich., Zürich, Switzerland, 1999. ???? pp. URL `http://e-collection.ethbib.ethz.ch/show?type=diss&nr=13106`; `http://www.de-moliner.ch/richard/thesis.html`.

Drossopoulou:1999:DSJ

[DE99] S. Drossopoulou and S. Eisenbach. Describing the semantics of Java and proving type soundness. *Lecture Notes in Computer Science*, 1523:41–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Deavours:1987:CPI

[Dea87] Cipher A. Deavours. *Cryptanalytic programs for the IBM PC*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1987. 44 pp.

Deavours:1988:BPS

[Dea88] Cipher A. Deavours. *Breakthrough '32: the Polish solution of the Enigma*, volume 51 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1988. ISBN 0-89412-152-9 (paperback). v + 85 pp. LCCN ????

Deavours:1998:A

[Dea98a] C. A. Deavours. The autoscritcher. In Deavours et al. [DKK+98], pages 541–552. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Kruh:1998:TBW

[Dea98b] Louis Kruh C. A. Deavours. The Turing bombe: was it enough? In Deavours et al. [DKK+98], pages 403–421. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Demirdogen:1988:FDM

[Dem88] A. Caner Demirdogen. Flaw detection methods based on digital signature analysis for rotating machinery quality control. Thesis (M.S.), Tennessee Technological University, Cookeville, TN, USA, 1988. xii + 189 pp.

Demytko:1994:NEC

[Dem94] N. Demytko. A new elliptic curve based analogue of RSA. *Lecture Notes in Computer Science*, 765:40–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650040.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650040.pdf`.

Denning:1979:SPC

[Den79a] Dorothy E. Denning. Secure personal computing in an insecure network. *Communications of the Association for Computing Machinery*, 22(8):476–482, August 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Denning:1979:EOS

[Den79b] Peter J. Denning. Editor's overview — special section on data encryption. *ACM Computing Surveys*, 11(4): 283, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Denning:1982:CDS

[Den82] Dorothy Elizabeth Robling Denning. *Cryptography and data security*. Addison-Wesley, Reading, MA, USA, 1982. ISBN 0-201-10150-5. xiii + 400 pp. LCCN QA76.9.A25 .D46 1982. US$22.95.

Denning:1984:DSR

[Den84a] Dorothy E. Denning. Digital signatures with RSA and other public-key cryptosystems. *Communications of the Association for Computing Machinery*, 27(4):388–392, April 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Denning:1984:FEA

[Den84b] Dorothy E. Denning. Field encryption and authentication. In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 231–247. Plenum Press, New York, NY, USA; London, UK, 1984.

Denniston:1986:GCC

[Den86] A. G. Denniston. The Government Code and Cypher School between the Wars. *Intelligence and National Security*, 1(1):48–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Denning:1990:DES

[Den90] Dorothy Denning. Data Encryption Standard: fifteen years of public scrutiny, 1990.

Denning:1995:ESC

[Den95] Dorothy Elizabeth Robling Denning. Encryption is a sword that cuts two ways, 1995. 1 videocassette (42 min.).

Denning:1999:IWS

[Den99] Dorothy Elizabeth Robling Denning. *Information warfare and security*. Addison-Wesley and ACM Press, Reading, MA, USA and New York, NY 10036, USA, 1999. ISBN 0-201-43303-6. xvii + 522 pp. LCCN U163.D46 1999. US$34.95.

Deswarte:1992:CSE

[DEQ92] Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, editors. *Computer security, ESORICS 92: Second European Symposium on Research in Computer Security, Toulouse, France, November 23–25, 1992: proceedings*, volume 648 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. CODEN LNCSD9. ISBN 3-540-56246-X (Berlin), 0-387-56246-X (New York). ISSN

0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E973 1992.

Desmedt:1988:SGC

[Des88] Y. Desmedt. Society and group-oriented cryptography: a new concept. In Pomerance [Pom88], pages 120–127. CODEN LNCSD9. ISBN 0-387-18796-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1987; QA267.A1 L43 no.293. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0293.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=293. CRYPTO '87, a Conference on the Theory and Applications of Cryptographic Techniques, held at the University of California, Santa Barbara ... August 16–20, 1987.

Desmedt:1990:PAA

[Des90a] Yvo Desmedt. Protecting against abuses of cryptosystems in particular in the context of verification of peace treaties (extended abstract). In *Sequences (Naples/Positano, 1988)*, pages 394–405. Springer, New York, 1990.

Desmedt:1990:MCS

[Des90b] Yvo G. Desmedt. Making conditionally secure cryptosystems unconditionally abuse-free in a general context (extended abstract). *Lecture Notes in Computer Science*, 435:6–16, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1992:BTC

[Des92] Yvo Desmedt. Breaking the traditional computer security research barriers. *Lecture Notes in Computer Science*, 648:125–138, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/021114.html.

Desmedt:1993:TC

[Des93] Y. Desmedt. Threshold cryptosystems. *Lecture Notes in Computer Science*, 718:3–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1994:TC

[Des94a] Y. Desmedt. Threshold cryptography. *European Transactions on Telecommunications: ETT*, 5(4): 449–457, July 1994. CODEN ETTTET. ISSN 1124-318X (print), 1541-8251 (electronic).

Desmedt:1994:ACC

[Des94b] Yvo G. Desmedt, editor. *Advances in cryptology, CRYPTO '94: 14th annual international cryptology conference, Santa Barbara, California, USA, August 21–25, 1994: proceedings*, volume 839 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0839.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=839`.

Desmedt:1995:STC

[Des95] Yvo Desmedt. Securing traceability of ciphertexts — towards a secure software key escrow system. *Lecture Notes in Computer Science*, 921:147–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210147.htm; http://link.springer-ny.com/link/service/series/0558/papers/0921/09210147.pdf`.

Desmedt:1996:EBB

[Des96a] Y. Desmedt. Establishing Big Brother using covert channels and other covert techniques. In Anderson [And96c], pages 65–71. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054327.html`.

Desmedt:1996:SPF

[Des96b] Yvo Desmedt. Simmons' protocol is not free of subliminal channels. In IEEE [IEE96c], pages 170–175. CODEN PCSWEZ. ISBN 0-8186-7522-5. ISSN 1063-6900. LCCN QA 76.9 A25 C655 1996. IEEE catalog number 96TB100047.

Desel:1998:BLA

[Des98a] J. Desel. Basic linear algebraic techniques for place/transition nets. *Lecture Notes in Computer Science*, 1492:257–308, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1998:C

[Des98b] Y. Desmedt. Crypto '94. *Lecture Notes in*

Computer Science, 1440: 173–180, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1998:SRR

[Des98c] Y. Desmedt. Some recent research aspects of threshold cryptography. *Lecture Notes in Computer Science*, 1396:158–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desfray:1999:ADP

[Des99a] P. Desfray. Automation of design pattern: Concepts, tools and practices. *Lecture Notes in Computer Science*, 1618:120–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1999:ES

[Des99b] Yvo Desmedt. Encryption schemes. In Atallah [Ata99], pages 39–1–39–28. ISBN 0-8493-2649-4. LCCN QA76.9.A43A43 1999.

Deugo:1997:CTS

[Deu97] Dwight Deugo. Coffee talk: From S390 mainframes to smart cards. *Java Report: The Source for Java Development*, 2(11):25–??, December 1997. CODEN JREPFI. ISSN 1086-4660.

Deugo:1998:SMS

[Deu98] Dwight Deugo. From S390 mainframes to smart cards. *Java Report: The Source for Java Development*, 3 (1):??, January 1998. CODEN JREPFI. ISSN 1086-4660. URL `http://archive.javareport.com/9808/html/features/archive/9801/coffeetalk.shtml`.

Desmedt:1990:TC

[DF90] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In Brassard [Bra90c], pages 307–315. CODEN LNCSD9. ISBN 0-387-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435`. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Desmedt:1991:SGA

[DF91a] Yvo Desmedt and Yair Frankel. Shared generation of authenticators and signatures (extended abstract). In Feigenbaum [Fei91], pages 457–469. CODEN LNCSD9. ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). ISSN

0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1991. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760457.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0576/05760457.pdf`. Conference held Aug. 11–15, 1991, at the University of California, Santa Barbara.

Domingo-Ferrer:1991:DUI

[DF91b] Josep Domingo-Ferrer. Distributed user identification by zero-knowledge access rights proving. *Information Processing Letters*, 40 (5):235–239, December 13, 1991. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Domingo-Ferrer:1991:SRT

[DF91c] Josep Domingo-Ferrer. Software run-time protection: a cryptographic issue. *Lecture Notes in Computer Science*, 473:474–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730474.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0473/04730474.pdf`.

Dawid:1992:BSC

[DF92] H. Dawid and G. Fettweis. Bit-level systolic carry-save array division. In *GLOBECOM '92. Communication for Global Users. IEEE Global Telecommunications Conference. Conference Record*, pages 484–488 (vol. 1). IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-7803-0608-2 (softbound), 0-7803-0609-0 (casebound), 0-7803-0610-4 (microfiche). LCCN TK5101.A1 I243 1992. Three volumes. IEEE catalog no. 92CH3130-2.

Desmedt:1993:PZS

[DF93] Y. Desmedt and Y. Frankel. Perfect zero-knowledge sharing schemes over any finite Abelian group. In R. Capocelli, A. De Santis, and U. Vaccaro, editors, *Sequences II: Methods in Communication, Security, and Computer Science*, pages 369–378. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993.

Domingo-Ferrer:1997:MAS

[DF97] Josep Domingo-Ferrer. Multi-application smart cards and encrypted data, processing. *Future Generation Computer Systems*, 13(1): 65–74, June 20, 1997. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.elsevier.com/gej-ng/10/19/19/28/17/21/abstract.html.

Domingo-Ferrer:1998:AFE

[DF98] J. Domingo-Ferrer. Anonymous fingerprinting of electronic information with automatic identification of redistributors. *Electronics Letters*, 34(13):1303–1304, June 25, 1998. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073122.html.

Domingo-Ferrer:1999:AFB

[DF99] J. Domingo-Ferrer. Anonymous fingerprinting based on committed oblivious transfer. *Lecture Notes in Computer Science*, 1560:43–52, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Deshpande:1999:VEM

[DFGH99] V. Deshpande, L. Fornasier, E. A. Gerteisen, and N. Hilbrink. Virtual engineering of multi-disciplinary applications and the significance of seamless accessibility of geometry data. *Lecture Notes in Computer Science*, 1593:702–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Domingo-Ferrer:1991:CTP

[DFHR91] J. Domingo-Ferrer and L. Huguet-Rotger. A cryptographic tool for programs protection. *Lecture Notes in Computer Science*, 514:227–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DiCrescenzo:1999:HFS

[DFIJ99] Giovanni Di Crescenzo, Niels Ferguson, Russell Impagliazzo, and Markus Jakobsson. How to forget a secret. *Lecture Notes in Computer Science*, 1563:500–509, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1563/15630500.htm; http://link.springer-ny.com/link/service/series/0558/papers/1563/15630500.pdf.

Dwork:1993:LCP

[DFKN93] C. Dwork, U. Feige, J. Kilian, and M. Naor. Low communication 2-Prover zero-knowledge proofs for NP. *Lecture Notes in Computer Science*, 740:215–227, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ding-Feng:1999:CS

[DFKYZD99] Ye Ding-Feng, Lam Kwok-Yan, and Dai Zong-Duo. Cryptanalysis of “2R” schemes. *Lecture Notes in Computer Science*, 1666: 315–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660315.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660315.pdf.

Donatini:1999:DES

[DFL99] P. Donatini, P. Frosini, and C. Landi. Deformation energy for size functions. *Lecture Notes in Computer Science*, 1654:44–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Davida:1997:ACC

[DFTY97] G. Davida, Y. Frankel, Y. Tsiounis, and M. Yung. Anonymity control in E-cash systems. In Hirschfeld [Hir97], pages 1–16. CODEN LNCSD9. ISBN 3-540-63594-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/071407.html.

Davison:1957:SCG

[DG57] W. H. T. Davison and M. Gordon. Sorting for chemical groups using Gordon–Kendall–Davison ciphers. *American Documentation*, 8(3):202–210, July 1957. CODEN AMDOA7. ISSN 0096-946X.

Davis:1995:KSC

[DG95] Don Davis and Daniel E. Geer. Kerberos security with clocks adrift. In USENIX Association [USE95b], pages 35–40. ISBN 1-880446-70-7. LCCN QA76.8.U65 U55 1992(3)-1995(5). URL http://www.usenix.org/publications/library/proceedings/security95/davis.html.

Dawson:1996:CPA

[DG96] Ed (Edward) Dawson and Jovan Golic, editors. *Cryptography: policy and algorithms: international conference, Brisbane, Queensland, Australia, July 3–5, 1995: proceedings*, volume 1029 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-60759-5 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C844 1996.

Davis:1996:KCAa

[DGT96] Donald T. Davis, Daniel E. Geer, and Theodore Ts'o. Kerberos with clocks adrift: History, protocols, and implementation. *Computing Systems*, 9(1):29–46, Winter 1996. CODEN CMSYE2. ISSN 0895-6340.

Daemen:1992:HDM

[DGV92] Joan Daemen, Rene Govaerts, and Joos Vandewalle. A hardware design model for cryptographic algorithms. *Lecture Notes in Computer Science*, 648: 419–??, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Daemen:1993:FDO

[DGV93] Joan Daemen, Rene Govaerts, and Joos Vandewalle. A framework for the design of one-way hash functions including cryptanalysis of Damgård's one-way function based on a cellular automaton. *Lecture Notes in Computer Science*, 739:82–96, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Daemen:1994:NAB

[DGV94a] J. Daemen, R. Govaerts, and J. Vandewalle. A new approach to block cipher design. *Lecture Notes in Computer Science*, 809:18–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Daemen:1994:RWS

[DGV94b] J. Daemen, R. Govaerts, and J. Vandewalle. Resynchronization weaknesses in synchronous stream ciphers. *Lecture Notes in Computer Science*, 765:159–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Daemen:1994:WKI

[DGV94c] Joan Daemen, Rene Govaerts, and Joos Vandewalle. Weak keys for IDEA. *Lecture Notes in Computer Science*, 773:224–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Diffie:1976:CPD

[DH76a] Whitfield Diffie and Martin E. Hellman. A critique of the proposed Data Encryption Standard. *Communications of the Association for Computing Machinery*, 19(3):164–165, March 1976. URL `https://dl.acm.org/doi/pdf/10.1145/360018.360031`.

Diffie:1976:NDC

[DH76b] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November 1976. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL `https://ee.stanford.edu/~hellman/publications/24.pdf`.

Diffie:1976:PKC

[DH76c] Whitfield Diffie and Martin E. Hellman. Public key cryptography. In IEEE, editor, *IEEE International Symposium on Information Theory, June 21–24, 1976, Ronneby, Sweden*, page ?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1976.

Diffie:1977:ECN

[DH77] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the NBS Data Encryption Standard. *Computer*, 10(6):74–84, June 1977. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Davis:1985:NRI

[DH85a] J. A. Davis and D. B. Holdridge. New results on integer factorizations. *Congressus Numerantium*, 46: 65–78, 1985. ISSN 0384-9864. Proceedings of the fourteenth Manitoba conference on numerical mathematics and computing (Winnipeg, Man., 1984).

Davis:1985:UFS

[DH85b] J. A. Davis and D. B. Holdridge. An update on factorization at Sandia National Laboratories. In Blakley and Chaum [BC85], page 114. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=114`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

DomingoiFerrer:1990:FSK

[DH90] Josep Domingo i Ferrer and Llorenç Huguet i Rotger. Full secure key exchange and authentication with no previously shared secrets. *Lecture Notes in Computer Science*, 434: 665–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/`

bibs/0434/04340665.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340665.pdf.

Dawson:1996:AAS

[DH96a] E. Dawson and J. He. Another approach to software key escrow encryption. *Lecture Notes in Computer Science*, 1172:87–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ding:1996:WKA

[DH96b] Yun Ding and Patrick Horster. Why the Kuperee authentication system fails. *Operating Systems Review*, 30(2):42–51, April 1996. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Dhem:1998:DEP

[Dhe98] J. F. Dhem. *Design of an efficient public-key cryptographic library for RISC-based smart cards*. Thesis (Ph.D.), University College London, London, UK, 1998.

Diffie:1980:CAM

[DHM80] B. W. Diffie, M. E. Hellman, and R. C. Merkle. Cryptographic apparatus and method. US Patent No. 4,200,770A., April 29, 1980. URL https://www.google.com/patents/US4200770. Patent filed 6 September 1977.

Dechamboux:1996:ADS

[DHMR96] P. Dechamboux, D. Hagimont, J. Mossiere, and X. Rousset de Pina. The Arias distributed shared memory: An overview. *Lecture Notes in Computer Science*, 1175:56–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1998:AOC

[DHQ98a] Y. Desmedt, S. Hou, and J.-J. Quisquater. Audio and optical cryptography. *Lecture Notes in Computer Science*, 1514:392–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1998:CC

[DHQ98b] Y. G. Desmedt, S. Hou, and J.-J. Quisquater. Cerebral cryptography. *Lecture Notes in Computer Science*, 1525:62–72, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dolev:1995:DFT

[DHSS95] Danny Dolev, Joseph Y. Halpern, Barbara Simons, and Ray Strong. Dynamic fault-tolerant clock synchronization. *Journal of the Association for Computing Machinery*, 42(1):143–

185, January 1995. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/200870.html`.

Damm:1995:MFH

[DHW95a] F. Damm, F.-P. Heider, and G. Wambach. MIMD-factorisation on hypercubes. *Lecture Notes in Computer Science*, 950: 400–409, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500400.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0950/09500400.pdf`.

Damm:1995:MH

[DHW95b] F. Damm, F.-P. Heider, and G. Wambach. MIMD-factorisation on hypercubes. *Lecture Notes in Computer Science*, 950: 400–409, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DiGiorgio:1997:ISC

[Di 97a] Rinaldo Di Giorgio. Interview: Smart card guru answers questions. *JavaWorld: IDG's magazine for the Java community*, 2(12): ??, December 1997. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/jw-12-1997/jw-12-javadev.interview.htm`.

DiGiorgio:1997:JDJ

[Di 97b] Rinaldo Di Giorgio. Java developer: Java smart card primer. *JavaWorld: IDG's magazine for the Java community*, 2(12):??, December 1997. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/jw-12-1997/jw-12-javadev.htm`.

DiCrescenzo:1999:SAC

[Di 99] Giovanni Di Crescenzo. *Security amplification of cryptographic primitives*. Thesis (Ph.D.), University of California, San Diego, San Diego, CA, USA, 1999.

DiCrescenzo:1999:SPH

[DI99] Giovanni Di Crescenzo and Russell Impagliazzo. Security-preserving hardness-amplification for any regular one-way function. In ACM [ACM99b], pages 169–178. ISBN 1-58113-067-8. LCCN QA75.5 .A14 1999. URL `http://www.acm.org/pubs/articles/proceedings/stoc/301250/p169-di_crescenzo/p169-di_crescenzo.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/301250/`

p169-di_crescenzo/. ACM order number 508990.

DiazdeLeon:1991:PIE

[Dia91] Peter Joseph Diaz de Leon. A parallel implementation of an encryption coprocessor. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1991. viii + 69 pp.

Ding:1996:CRT

[DiDPS96] C. (Cunsheng) Ding, Ting i (Dingyi) P'ei, and Arto Salomaa. *Chinese remainder theorem: applications in computing, coding, cryptography*. World Scientific Publishing Co., Singapore; Philadelphia, PA, USA; River Edge, NJ, USA, 1996. ISBN 981-02-2827-9. viii + 213 pp. LCCN QA268.D55 1996.

Dieringer:1988:TAE

[Die88] Jeffrey A. Dieringer. Tools for analog encryption. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1988. vi + 93 pp.

Diffie:1975:PRN

[Dif75] Whitfield Diffie. Preliminary remarks on the National Bureau of Standards proposed standard encryption algorithm for computer data protection. Unpublished report, Stanford University, Stanford, CA, USA, May 1975.

Diffie:1982:CVP

[Dif82a] Whitfield Diffie. Conventional versus public key cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 41–72. Westview, Boulder, CO, 1982.

Diffie:1982:CTF

[Dif82b] Whitfield Diffie. Cryptographic technology: fifteen year forecast. *ACM SIGACT News*, 14(4):38–57, Fall–Winter 1982. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Diffie:1988:FTY

[Dif88] Whitfield Diffie. The first ten years of public-key cryptography. *Proceedings of the IEEE*, 76:560–576, 1988. CODEN IEEPAD. ISSN 0018-9219.

Diffie:1990:APK

[Dif90] Whitfield Diffie. The adolescence of public-key cryptography (invited). *Lecture Notes in Computer Science*, 434:2–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/

link/service/series/0558/bibs/0434/04340002.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340002.pdf.

Davis:1994:CRA

[DIF94] Don Davis, Ross Ihaka, and Philip Fenstermacher. Cryptographic randomness from air turbulence in disk drives. In Desmedt [Des94b], pages 114–120. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390114.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390114.pdf.

Ding:1994:DCD

[Din94] C. Ding. The differential cryptanalysis and design of natural stream ciphers. *Lecture Notes in Computer Science*, 809:101–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dixon:1994:SSS

[Dix94] Robert C. Dixon. *Spread spectrum systems: with commercial applications*. Wiley, New York, third edition, 1994. ISBN 0-471-59342-7. xv + 573 pp. LCCN TK5102.5 .D55 1994. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1010.html.

Damm:1998:CRT

[DJHP98] W. Damm, B. Josko, H. Hungar, and A. Pnueli. A compositional real-time semantics of STATEMATE designs. *Lecture Notes in Computer Science*, 1536:186–238, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dessmark:1993:MDD

[DJL93] A. Dessmark, K. Jansen, and A. Lingas. The maximum k-dependent and f-dependent set problem. *Lecture Notes in Computer Science*, 762:88–97, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Deavours:1985:MCM

[DK85] Cipher A. Deavours and Louis Kruh. *Machine cryptography and modern cryptanalysis*. The Artech House telecom library. Artech House Inc., Norwood, MA, USA, 1985. ISBN 0-89006-161-0. xiv + 258 pp. LCCN Z103 .D431 1985.

Deavours:1989:CMH

[DK+89] Cipher A. Deavours, David Kahn, et al., editors. *Cryptology: machines, history, & methods*. Artech House Inc., Norwood, MA, USA, 1989. ISBN 0-89006-399-0. x + 508 pp. LCCN Z103 .C75 1989. Second volume of selected papers from issues of Cryptologia.

Dusse:1991:CLM

[DK91] Stephen R. Dusse and Burt S. Kaliski Jr. A cryptographic library for the Motorola DSP56000. *Lecture Notes in Computer Science*, 473:230–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730230.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730230.pdf.

Damgaard:1994:BAH

[DK94] I. B. Damgård and L. R. Knudsen. The breaking of the AR hash function. *Lecture Notes in Computer Science*, 765:286–292, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Damgaard:1996:MEM

[DK96] I. B. Damgaard and L. R. Knudsen. Multiple encryption with minimum key. *Lecture Notes in Computer Science*, 1029:156–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Deavours:1998:SCH

[DKK+98] Cipher A. Deavours, David Kahn, Louis Kruh, Greg Mellen, and Brian J. Winkel, editors. *Selections From Cryptologia: History, People, And Technology*. The Artech House telecommunications library. Artech House Inc., Norwood, MA, USA, February 1998. ISBN 0-89006-862-3. vii + 552 pp. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Desmedt:1998:CES

[DKKK98] Y. Desmedt, B. King, W. Kishimoto, and K. Kurosawa. A comment on the efficiency of secret sharing scheme over any finite Abelian group. *Lecture Notes in Computer Science*, 1438:391–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Deavours:1987:CYT

[DKKM87] Cipher A. Deavours, David Kahn, Louis Kruh, and

Greg Mellen, editors. *Cryptology yesterday, today, and tomorrow*. The Artech House communication and electronic defense library. Artech House Inc., Norwood, MA, USA, 1987. ISBN 0-89006-253-6. xi + 519 pp. LCCN Z103.C76 1987. US$60.00. First volume of selected papers from issues of Cryptologia.

Daemen:1997:BCSb

[DKR97a] J. Daemen, L. Knudsen, and V. Rijmen. The block cipher square. *Lecture Notes in Computer Science*, 1267:149–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Daemen:1997:BCSa

[DKR97b] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher square algorithm: a fast block cipher that uses a 128-bit key. *Dr. Dobb's Journal of Software Tools*, 22(10): 54, 56–57, October 1997. CODEN DDJOEB. ISSN 1044-789X.

Dodson:1995:NFL

[DL95] B. Dodson and A. K. Lenstra. NFS with four large primes: An explosive experiment. In Coppersmith [Cop95d], page ?? CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=963`. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Dam:1996:CRS

[DL96] Kenneth W. Dam and Herbert Lin, editors. *Cryptography's role in securing the information society*. National Academy Press, Washington, DC, USA, 1996. ISBN 0-309-05475-3. xxx + 688 pp. LCCN TK5102.94 .C78 1996. US$44.95. Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council.

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. ix + 342 pp. LCCN KF9670 .D54 1998.

Demphlous:1999:DPL

[DL99] S. Demphlous and F. Lebastard. Designing persistence libraries in reflective models with intercession property for a client-server environment. *Lecture Notes in Computer Science*, 1616:54–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Davoine:1997:VCP

[DLF97] F. Davoine, H. Li, and R. Forchheimer. Video compression and person authentication. *Lecture Notes in Computer Science*, 1206: 353–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeMillo:1982:CP

[DLM82] Richard A. DeMillo, Nancy A. Lynch, and Michael J. Merritt. Cryptographic protocols. In ACM [ACM82], pages 383–400. ISBN 0-89791-070-2. LCCN QA75.5 .A14 1982. ACM order no. 508820.

Damgaard:1993:ACE

[DLP93] Ivan Damgård, Peter Landrock, and Carl Pomerance. Average case error estimates for the strong probable prime test. *Mathematics of Computation*, 61 (203):177–194, July 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Ding:1997:LMS

[DLR97] C. Ding, T. Laihonen, and A. Renvall. Linear multisecret-sharing schemes and error-correcting codes. *J.UCS: Journal of Universal Computer Science*, 3(9):1023–1036, September 28, 1997. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL `http://medoc.springer.de:8000/jucs/jucs_3_9/linear_multisecret_sharing`.

delaStelle:1902:TCF

[dlS02] Félix-Marie de la Stelle. *Traité de cryptographie. (French) [Treatise on cryptography]*. Gauthier-Villars, Paris, France, 1902. ???? pp.

DeMillo:1983:PDS

[DM83] R. DeMillo and M. Merritt. Protocols for data security. *Computer*, 16 (2):39–50, February 1983. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1004.html`.

Duc:1997:PAF

[DMFB97] B. Duc, G. Maitre, S. Fischer, and J. Bigun. Person authentication by fusing face and speech information. *Lecture Notes in Computer Science*, 1206: 311–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeWin:1998:PSS

[DMPW98] E. De Win, S. Mister, B. Preneel, and M. Wiener. On the performance of signature schemes based on elliptic curves. *Lecture Notes in Computer Science*, 1423: 252–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Denning:1981:MMK

[DMS81] D. E. Denning, H. Meijer, and F. B. Schneider. More on master keys for group sharing. *Information Processing Letters*, 13(3):125–126, December 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Dongarra:1995:TSS

[DMS95] J. J. Dongarra, H. W. Meuer, and E. Strohmaier. TOP500 supercomputer sites. *Supercomputer*, 11(2-3):133–163 (or 164–194??), June 1995. CODEN SPCOEL. ISSN 0168-7875. URL `http://www.netlib.org/benchmark/top500.html`.

Denazis:1999:DIO

[DMVC99] S. Denazis, K. Miki, J. Vicente, and A. Campbell. Designing interfaces for open programmable routers. *Lecture Notes in Computer Science*, 1653: 13–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DAngelo:1994:SEM

[DMW94] Diana M. D'Angelo, Bruce McNair, and Joseph E. Wilkes. Security in electronic messaging systems. *AT&T Technical Journal*, 73(3):7–13, 1994. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Dwork:1993:PPC

[DN93] C. Dwork and M. Naor. Pricing via processing or combatting junk mail. *Lecture Notes in Computer Science*, 740:139–147, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dwork:1994:EEU

[DN94] Cynthia Dwork and Moni Naor. An efficient existentially unforgeable signature scheme and its applications. In Desmedt

[Des94b], pages 234–246. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390234.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390234.pdf. To appear in J. of Crypto. Preliminary version in Proceedings of Crypto '94.

Dossis:1995:FSR

[DN95a] M. F. Dossis and J. M. Noras. Feasibility studies for RSA ASICS via multilevel simulation. In ????, editor, *7th European Simulation Symposium (ESS'95), October 26–28 1995, Erlangen-Nürnberg, Germany*, pages 416–427. ????, ????, 1995. ISBN ???? LCCN ????

Dossis:1995:OVH

[DN95b] M. F. Dossis and J. M. Noras. Optimising and verifying hardware algorithms for RSA public-key cryptography. Departmental Research Report 569, University of Bradford, Bradford, Yorkshire, UK, February 1995.

Ding:1997:TFS

[DNRS97] C. Ding, V. Niemi, A. Renvall, and A. Salomaa. TWOPRIME: a fast stream ciphering algorithm. *Lecture Notes in Computer Science*, 1267:88–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dittmann:1998:IWE

[DNSS98] Jana Dittmann, Frank Nack, Arnd Steinmetz, and Ralf Steinmetz. Interactive watermarking environments. In IEEE [IEE98e], pages 286–294. ISBN 0-8186-8557-3, 0-8186-8559-X (microfiche). LCCN QA76.575.I623 1998. IEEE catalog number 98TB100241. IEEE Computer Society Order Number PR08557.

Desmedt:1986:CTA

[DO86] Y. G. Desmedt and A. M. Odlyzko. A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes. In Williams [Wil86b], pages 516–522. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL http://www.research.att.com/~amo/doc/arch/rsa.attack.pdf; http://www.research.att.com/~amo/doc/arch/rsa.attack.ps; http://www.research.att.com/~amo/doc/arch/rsa.attack.troff.

DiCrescenzo:1999:CZK

[DO99] G. Di Crescenzo and R. Ostrovsky. On concurrent zero-knowledge with preprocessing. *Lecture Notes in Computer Science*, 1666: 485–502, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dobbertin:1995:EMC

[Dob95a] H. Dobbertin. Extended MD4 compress is not collision-free. Unpublished abstract., October 1995.

Dobbertin:1995:ASA

[Dob95b] Hans Dobbertin. Alf swindles Ann. *CryptoBytes*, 1 (3):5, Autumn 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf`.

Dobbertin:1996:CM

[Dob96a] H. Dobbertin. Cryptanalysis of MD4. In Gollmann [Gol96d], pages 53–69. CODEN LNCSD9. ISBN 3-540-60865-6 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F38 1996. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1039.htm`; `http://www.springerlink.com/content/978-3-540-60865-3`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1039`.

Dobbertin:1996:SMA

[Dob96b] Hans Dobbertin. The status of MD5 after a recent attack. *CryptoBytes*, 2(2): 1, 3–6, Summer 1996. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto2n2.pdf`.

Dobbertin:1997:RTC

[Dob97] H. Dobbertin. RIPEMD with two-round compress function is not collision-free. *Journal of Cryptology*, 10(1):51–69, Winter 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/bibs/10n1p51.html`; `http://link.springer.de/link/service/journals/00145/bibs/10n1p51.pdf`; `http://link.springer.de/link/service/journals/00145/bibs/10n1p51.tex`; `http://link.springer.de/link/service/journals/00145/tocs/01001.html`.

Dobbertin:1998:FTR

[Dob98] H. Dobbertin. The first two rounds of MD4 are not one-way. In Vaudenay [Vau98e], page ?? CODEN LNCSD9. ISBN 3-540-64265-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN

QA76.9.A25F77 1998. To appear.

Dobbertin:19xx:CM

[Dobxx] H. Dobbertin. Cryptanalysis of MD4. Submitted to Journal of Cryptology., 19xx.

DomingoiFerrer:1996:NPH

[Dom96] Josep Domingo i.Ferrer. A new privacy homomorphism and applications. *Information Processing Letters*, 60 (5):277–282, December 8, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Donini:1998:CSR

[Don98] Luigi Donini. The cryptographic services of the Royal (British) and Italian navies: a comparative analysis of their activities during World War II. In Deavours et al. [DKK+98], pages 3–33. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

DiCrescenzo:1999:COTb

[DOR99] Giovanni Di Crescenzo, Rafail Ostrovsky, and Sivaramakrishnan Rajagopalan. Conditional oblivious transfer and timed-release encryption. In *Advances in cryptology—EUROCRYPT '99 (Prague)*, volume 1592 of *Lecture Notes in Computer Science*, pages 74–89. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920074.htm; http://link.springer-ny.com/link/service/series/0558/papers/1592/15920074.pdf`.

Santis:1991:PRP

[DP91] Alfredo De Santis and Giuseppe Persiano. Public-randomness in public-key cryptography (extended abstract). *Lecture Notes in Computer Science*, 473: 46–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730046.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730046.pdf`.

DiCrescenzo:1994:ROP

[DP94] Giovanni Di Crescenzo and Giuseppe Persiano. Round-optimal perfect zero-knowledge proofs. *Information Processing Letters*, 50(2):93–99, April 22, 1994. CODEN IFPLAT. ISSN 0020-0190

(print), 1872-6119 (electronic).

Damgaard:1996:NCU

[DP96] I. Damgaard and T. P. Pedersen. New convertible undeniable signature schemes. *Lecture Notes in Computer Science*, 1070:372–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Davida:1998:HC

[DP98a] G. Davida and R. Peralta. High-speed cryptography. *Lecture Notes in Computer Science*, 1396:116–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Davida:1998:HSC

[DP98b] G. Davida and R. Peralta. High-speed cryptography. *Lecture Notes in Computer Science*, 1396:116–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeWin:1998:ECP

[DP98c] Erik De Win and Bart Preneel. Elliptic curve public-key cryptosystems — an introduction. *Lecture Notes in Computer Science*, 1528: 131–141, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1528/15280131.htm; http://link.springer-ny.com/link/service/series/0558/papers/1528/15280131.pdf`.

Descombes:1999:MVK

[DP99] X. Descombes and E. Pechersky. Metropolis vs Kawasaki dynamic for image segmentation based on Gibbs models. *Lecture Notes in Computer Science*, 1654:99–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeWaleffe:1993:BLP

[DQ93] D. De Waleffe and J.-J. Quisquater. Better login protocols for computer networks. *Lecture Notes in Computer Science*, 741: 50–70, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Delos:1994:IBS

[DQ94] Olivier Delos and Jean-Jacques Quisquater. An identity-based signature scheme with bounded life-span. In Desmedt [Des94b], pages 83–94. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-`

ny.com/link/service/series/0558/bibs/0839/08390083.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390083.pdf.

Desmedt:1985:DOI

[DQD85] Yvo Desmedt, Jean-Jacques Quisquater, and Marc Davio. Dependence of output on input in DES: Small avalanche characteristics. In Blakley and Chaum [BC85], pages 359–376. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=359. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

deRooij:1994:SPD

[dR94a] Peter de Rooij. On Schnorr's preprocessing for digital signature schemes. *Lecture Notes in Computer Science*, 765:435–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650435.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650435.pdf.

Rooij:1994:SPD

[dR94b] Peter de Rooij. On Schnorr's preprocessing for digital signature schemes. *Lecture Notes in Computer Science*, 765:435–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650435.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650435.pdf.

Desel:1994:PNR

[DR94c] J. Desel and M.-D. Radola. Proving non-reachability by modulo-place-invariants. *Lecture Notes in Computer Science*, 880:366–377, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

deRooij:1995:EEU

[dR95] Peter de Rooij. Efficient exponentiation using precomputation and vector addition chains. *Lecture Notes in Computer Science*, 950:389–399, 1995. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500389.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500389.pdf.

Daemen:1998:APR

[DR98a] J. Daemen and V. Rijmen. AES proposal: Rijndael. NIST AES Proposal, June 1998.

Desel:1998:PTP

[DR98b] J. Desel and W. Reisig. Place/transition Petri nets. *Lecture Notes in Computer Science*, 1492:122–173, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Daemen:1999:EBC

[DR99a] Joan Daemen and Vincent Rijmen. Efficient block ciphers for Smartcards. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL http://www.usenix.org/publications/library/proceedings/smartcard99/daemen.html.

Drea:1999:NEB

[DR99b] Edward J. Drea and Joseph E. Richard. New evidence on breaking the Japanese Army codes. *Intelligence and National Security*, 14 (1):62–??, 1999. ISSN 0268-4527 (print), 1743-9019 (electronic).

Dray:1998:RNJ

[Dra98] Jim Dray. Report on the NIST Java AES candidate algorithm analysis. In National Institute of Standards and Technology [Nat98], page 29. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/r1-java.pdf. See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

Drach:1999:RDO

[Dra99] S. Drach. RFC 2485: DHCP option for the Open Group's user authentication protocol, January 1999. URL ftp://ftp.internic.net/rfc/rfc2485.txt; https://www.math.utah.edu/pub/rfc/rfc2485.txt. Status: PROPOSED STANDARD.

Dreher:1979:PSC

[Dre79] Felix F. Dreher. Privacy and security in computer based systems using encryption. Pittsburg State

University. School of Business monograph series 7, Pittsburg State University. Gladys A. Kelce School of Business and Economics., Pittsburg, KS, USA, 1979. 8 pp.

Drea:1992:MUC

[Dre92] Edward J. Drea. *MacArthur's ULTRA: codebreaking and the war against Japan, 1942–1945*. Modern war studies. University Press of Kansas, Lawrence, KS, USA, 1992. ISBN 0-7006-0504-5, 0-7006-0576-2 (paperback). xv + 296 pp. LCCN D767 .D66 1992.

deRaadt:1999:COO

[dRHG+99] Theo de Raadt, Niklas Hallqvist, Artur Grabowski, Angelos D. Keromytis, and Niels Provos. Cryptography in OpenBSD: An overview. In USENIX [USE99d], page ?? ISBN 1-880446-33-2. LCCN ???? URL `http://www.openbsd.org/papers/crypt-paper.ps`.

Dror:1989:SCG

[Dro89] Asael Dror. Secret codes (any good data security system must rely on encryption). *BYTE Magazine*, 14(6):267–270, June 1989. CODEN BYTEDJ. ISSN 0360-5280.

Droste:1996:NRV

[Dro96] S. Droste. New results on visual cryptography. *Lecture Notes in Computer Science*, 1109:401–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dawson:1995:DIJ

[DRR95] S. Dawson, C. R. Ramakrishnan, and I. V. Ramakrishnan. Design and implementation of jump tables for fast indexing of logic programs. *Lecture Notes in Computer Science*, 982: 133–150, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Denning:1981:MKG

[DS81] Dorothy E. Denning and Fred B. Schneider. Master keys for group sharing. *Information Processing Letters*, 12(1):23–25, February 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See also note [Bv82].

Dolev:1983:AAB

[DS83] D. Dolev and H. R. Strong. Authenticated algorithms for Byzantine agreement. *SIAM Journal on Computing*, 12(4):656–666, ???? 1983. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Davis:1990:NSP

[DS90a] Don Davis and Ralph Swick. Network security via private-key certificates. *Operating Systems Review*, 24(4):64–67, October 1990. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Davis:1990:WSK

[DS90b] Don Davis and Ralph Swick. Workstation services and Kerberos authentication at Project Athena. Report MIT/LCS/TM 424, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1990. 8 pp.

Desmedt:1993:PPS

[DS93] Y. Desmedt and J. Seberry. Practical proven secure authentication with arbitration. *Lecture Notes in Computer Science*, 718:27–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Davern:1996:FBI

[DS96] P. Davern and M. Scott. Fractal based image steganography. *Lecture Notes in Computer Science*, 1174: 279–294, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054120.html.

Devanbu:1997:CVT

[DS97a] P. Devanbu and S. G. Stubblebine. Cryptographic verification of test coverage claims. *Lecture Notes in Computer Science*, 1301: 395–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dittmann:1997:ETT

[DS97b] J. Dittmann and A. Steinmetz. Enabling technology for the trading of MPEG-encoded video. In Varadharajan et al. [VPM97], pages 314–324. CODEN LNCSD9. ISBN 3-540-63232-8 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN A76.9.A25A279 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064124.html.

Dittmann:1997:TAT

[DS97c] J. Dittmann and A. Steinmetz. A technical approach to the transparent encryption of MPEG-2 video. In Katsikas [Kat97], pages 215–226. ISBN 0-412-81770-5. LCCN QA76.9.A25 I464 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064125.html.

Dutertre:1997:UPE

[DS97d] B. Dutertre and S. Schneider. Using a PVS embedding of CSP to verify authentication protocols. *Lecture Notes in Computer Science*, 1275:121–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

David:1998:SIC

[DS98a] M. W. David and K. Sakurai. Security issues for contactless smart cards. *Lecture Notes in Computer Science*, 1431:247–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dwork:1998:CZR

[DS98b] C. Dwork and A. Sahai. Concurrent zero-knowledge: Reducing the need for timing constraints. *Lecture Notes in Computer Science*, 1462:442–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Durham:1999:BOO

[DSB99] George B. Durham, Diomidis Spinelis, and Mariá Bieliková. Bookshelf: Object-oriented software design and construction with C++: Decrypted secrets: Methods and maxims of cryptology: Software engineering: Theory and practice. *IEEE Software*, 16(4):114–117, July/August 1999. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic). URL http://dlib.computer.org/so/books/so1999/pdf/s4114.pdf.

Dittmann:1998:RMV

[DSS98] J. Dittmann, M. Stabenau, and R. Steinmetz. Robust MPEG video watermarking technologies. In Effelsberg and Smith [ES98], pages 71–80. ISBN 1-58113-036-8. LCCN QA76.575.A36 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073121.html. ACM order number 43398.

Dave:1995:CBS

[DSSB95] B. Dave, G. Schmitt, S.-G. Shih, and L. Bendel. Case-based spatial design reasoning. *Lecture Notes in Computer Science*, 984:198–210, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desai:1999:CSC

[DSSZ99] B. C. Desai, R. Shinghal, N. Shayan, and Y. Zhou. CINDI: a system for cataloguing, searching, and annotating electronic documents in digital libraries. *Lecture Notes in Computer*

Science, 1609:154–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Durand:1999:DCC

[DSV99] B. Durand, A. Shen, and N. Vereshagin. Descriptive complexity of computable sequences. *Lecture Notes in Computer Science*, 1563: 153–162, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Detombe:1993:CLC

[DT93] J. Detombe and S. E. Tavares. Constructing large cryptographically strong S-boxes. *Lecture Notes in Computer Science*, 718: 165–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSolages:1998:EFO

[DT98a] A. De Solages and J. Traore. An efficient fair off-line electronic cash system with extensions to checks and wallets with observers. *Lecture Notes in Computer Science*, 1465:275–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DiGiorgio:1998:JDS

[DT98b] Rinaldo Di Giorgio and Peter Trommler. Java developer: Smart cards and the OpenCard Framework. *JavaWorld: IDG's magazine for the Java community*, 3(1):??, January 1998. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/jw-01-1998/jw-01-javadev.html`.

DuBoulay:1999:DDT

[DTDJ99] B. Du Boulay, B. Teather, G. Du Boulay, and N. Jeffrey. From description to decision: Towards a decision support training system for MR radiology of the brain. *Lecture Notes in Computer Science*, 1620:93–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

duCarlet:1644:CCV

[du 44] Maistre Iean Robert du Carlet. *La cryptographie: contenant vne tres-subtile manier d'escrire secrètement. (French) [Cryptography: containing a very subtle manner of secret writing]*. Imprimeur ordinaire du Roy et R. Aurelhe, Marchand libraire, Paris, France, 1644. 234 + 2 pp. LCCN Z103.5 .D82 1644b.

Dufner:1998:ACH

[Duf98] Mark S. Dufner. Applications of cryptology in high school mathematics. Thesis (M.A.), Minot State University, 500 University Ave.

West Minot, ND 58707, USA, 1998. vii + 113 pp.

Duhoux:1990:DBA

[Duh90] Yves Duhoux. Deciphering Bronze Age scripts of Crete — the case of Linear A (invited). *Lecture Notes in Computer Science*, 434:649–650, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340649.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340649.pdf`.

Dumey:1994:CQD

[Dum94] Arnold I. Dumey. Comments, queries, and debate: Scritchers. *IEEE Annals of the History of Computing*, 16(3):4, Fall 1994. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL `http://dlib.computer.org/an/books/an1994/pdf/a3004.pdf`.

deVivo:1998:ISA

[dVdVI98] Marco de Vivo, Gabriela O. de Vivo, and Germinal Isern. Internet security attacks at the basic levels. *Operating Systems Review*, 32(2):4–15, April 1998. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

DeDecker:1992:HID

[DVPL92] Bart De Decker, Els Van Herreweghen, Frank Piessens, and K. U. Leuven. Heterogeneous intra-domain authentication. In USENIX [USE92b], pages 285–298. ISBN 1-880446-46-4. LCCN ????

Dhem:1996:SSC

[DVQ96] Jean-François Dhem, Daniel Veithen, and Jean-Jacques Quisquater. SCALPS: Smart Card for Limited Payment Systems — merging a processor and a coprocessor on a fast, secure, low-cost chip dedicated to public-key cryptography. *IEEE Micro*, 16(3):42–51, May/June 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

DeSoete:1990:CAS

[DVW90] Marijke De Soete, Klaus Vedder, and Michael Walker. Cartesian authentication schemes. *Lecture Notes in Computer Science*, 434:476–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340476.htm; http://link.springer-`

ny.com/link/service/series/0558/papers/0434/04340476.pdf.

Diffie:1992:AAK

[DvW92] Whitfield Diffie, Paul C. van Oorschot, and Michael J. Wiener. Authentication and authenticated key exchanges. *Designs, Codes, and Cryptography*, 2(2):107–125, June 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

DiPorto:1994:VBC

[DW94] A. Di Porto and W. Wolfowicz. VINO: a block cipher including variable permutations. *Lecture Notes in Computer Science*, 809: 205–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Danielsson:1998:HKW

[DW98] Johan Danielsson and Assar Westerlund. Heimdal — Kerberos 5 for the world (slides). In USENIX [USE98c], page ?? ISBN ???? LCCN ???? URL http://www.usenix.org/publications/library/proceedings/usenix98/freenix/heimdal1.ps.

Davida:1981:DES

[DWK81] George I. Davida, David L. Wells, and John B. Kam. A database encryption system with subkeys. *ACM Transactions on Database Systems*, 6(2):312–328, June 1981. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL http://www.acm.org/pubs/articles/journals/tods/1981-6-2/p312-davida/p312-davida.pdf; http://www.acm.org/pubs/citations/journals/tods/1981-6-2/p312-davida/.

Dwork:1991:VSS

[Dwo91] Cynthia Dwork. On verification in secret sharing. *Lecture Notes in Computer Science*, 576:114–128, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dwork:1995:DCC

[Dwo95] Cynthia Dwork. Distributed computing column: Lotus Notes security and authentication. *ACM SIGACT News*, 26(1):17–19, March 1995. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Dwork:1997:PAL

[Dwo97] C. Dwork. Positive applications of lattices to cryptography. *Lecture Notes in Computer Science*, 1295: 44–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

deWaleffe:1991:CSC

[dWQ91a] Dominique de Waleffe and Jean-Jacques Quisquater. CORSAIR: a smart card for public key cryptosystems. *Lecture Notes in Computer Science*, 537: 502–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370502.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370502.pdf.

Waleffe:1991:CSC

[dWQ91b] Dominique de Waleffe and Jean-Jacques Quisquater. CORSAIR: a smart card for public key cryptosystems. In Menezes and Vanstone [MV91], pages 503–513. CODEN LNCSD9. ISBN 0-387-54508-5 (New York), 3-540-54508-5 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1990. URL http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370502.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370502.pdf. Conference held Aug. 11–15, 1990, at the University of California, Santa Barbara.

Dai:1996:CFA

[DWZ96] Dawei Dai, Kui Wu, and Huanguo Zhang. Cryptanalysis on a finite automaton public key cryptosystem. *Science in China. Series E, Technological sciences*, 39(1):27–36, 1996. CODEN SCETFO. ISSN 1006-9321 (print), 1862-281X (electronic).

Ding:1991:STS

[DXS91] C. (Cunsheng) Ding, G. Xiao, and W. Shan. *The stability theory of stream ciphers*, volume 561 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. CODEN LNCSD9. ISBN 3-540-54973-0 (Berlin), 0-387-54973-0 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). ix + 187 pp. LCCN QA402.3 .D536 1991.

DeSantis:1990:DPS

[DY90] A. De Santis and M. Yung. On the design of provably-secure cryptographic hash functions. In Damgård [Dam90a], pages 377–397. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). LCCN QA76.9.A25 E964 1990. DM69.00.

DeSantis:1991:CAN

[DY91a] A. De Santis and M. Yung. Cryptographic applications of the non-interactive metaproofs and many-prover systems. *Lecture Notes in Computer Science*, 537:366–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSantis:1991:DPSb

[DY91b] A. De Santis and M. Yung. On the design of provably-secure cryptographic hash functions. In Damgård [Dam91a], pages 377–397. CODEN LNCSD9. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1990. DM69.00.

Santis:1991:CAN

[DY91c] Alfredo De Santis and Moti Yung. Cryptographic applications of the non-interactive metaproof and many-prover systems (preliminary version). *Lecture Notes in Computer Science*, 537:366–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370366.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370366.pdf`.

DeSantis:1991:DPSa

[DY91d] Alfredo De Santis and Moti Yung. On the design of provably-secure cryptographic hash functions (extended summary). *Lecture Notes in Computer Science*, 473:412–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730412.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730412.pdf`.

Desmedt:1991:WUS

[DY91e] Y. Desmedt and M. Yung. Weaknesses of undeniable signature schemes. *Lecture Notes in Computer Science*, 547:205–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1991:AUS

[DY91f] Yvo Desmedt and Moti Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks (extended abstract). *Lecture Notes in Computer Science*, 537: 177–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370177.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370177.pdf.

Dai:1998:WIF

[DYL98] ZongDuo Dai, Ding Feng Ye, and Kwok Yan Lam. Weak invertibility of finite automata and cryptanalysis on FAPKC. *Lecture Notes in Computer Science*, 1514:227–241, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Eberle:1993:HSI

[Ebe93] H. Eberle. A high-speed DES implementation for network applications. *Lecture Notes in Computer Science*, 740:521–539, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Easter:1999:PES

[ECD+99] R. J. Easter, E. W. Chencinski, E. J. D'Avignon, S. R. Greenspan, W. A. Merz, and C. D. Norberg. S/390 Parallel Enterprise Server CMOS cryptographic coprocessor. *IBM Journal of Research and Development*, 43(5/6):761–776, ???? 1999. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL http://www.research.ibm.com/journal/rd/435/easter.html.

Ecker:1982:MGE

[Eck82] A. Ecker. Über die mathematischen Grundlagen einiger Chiffrierverfahren. (German) [On the mathematical foundations of some cryptosystems]. *Computing*, 29(4):277–287, 1982. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Ecker:1983:FSR

[Eck83] A. Ecker. Finite semigroups and the RSA-cryptosystem. *Lecture Notes in Computer Science*, 149:353–369, 1983. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ecker:1985:STS

[Eck85] Allen Ecker. Satellite television, signal encryption and the future of broadband distribution. Seminar notes, Communications Forum, Massachusetts Institute of Technology, Cambridge, MA, USA, September 19, 1985. 13 pp.

ECMA:1996:EAP

[ECM96] ECMA. *ECMA-219: Authentication and Privilege*

Attribute Security Application with Related Key Distribution Functions — Part 1, 2 and 3. ECMA (European Association for Standardizing Information and Communication Systems), Geneva, Switzerland, second edition, March 1996. URL http://www.ecma.ch/ecma1/STAND/ECMA-219.HTM.

Ellis:1975:PKC

[ECW75] James Ellis, Clifford Cocks, and Malcolm Williamson. Public-key cryptography. Classified reports (titles uncertain) at Government Communications Headquarters (GCHQ), Cheltenham, UK., 1975. URL http://www.gchq.gov.uk/Press/Pages/100th-IEEE-milestone-award.aspx. Work declassified in 1997. Awarded the 100th IEEE Milestone Award for the first discovery (albeit long secret) of public-key cryptography.

Edwards:1915:CCT

[Edw15] E. C. Edwards. Cipher codes and their uses. *Scientific American*, 113(1): 9, July 3, 1915. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v113/n1/pdf/scientificamerican07031915-9.pdf.

Epstein:1956:FBC

[EE56] Sam Epstein and Beryl Epstein. *The first book of codes and ciphers*. Franklin Watts, New York, NY, USA, 1956. LCCN Z104 .E68. Pictures by Laszlo Roth.

El-Gamal:1985:PCS

[EG85a] T. El-Gamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31(4):469–472, 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Even:1985:PCC

[EG85b] S. Even and O. Goldreich. On the power of cascade ciphers. *ACM Transactions on Computer Systems*, 3(2):108–116, May 1985. CODEN ACSYEC. ISSN 0734-2071. URL http://www.acm.org:80/pubs/citations/journals/tocs/1985-3-2/p108-even/.

Even:1985:RPS

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the Association for Computing Machinery*, 28(6):637–647, June 1985. CODEN

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/3818.html.

Even:1990:LLD

[EGM90] Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. *Lecture Notes in Computer Science*, 435: 263–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350263.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350263.pdf.

Even:1996:LLD

[EGM96] Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. *Journal of Cryptology*, 9(1):35–67, Winter 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n1p35.html; http://link.springer.de/link/service/journals/00145/bibs/9n1p35.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n1p35.tex; http://link.springer.de/link/service/journals/00145/tocs/00901.html.

English:1996:NSU

[EH96] Erin English and Scott Hamilton. Network security under siege: The timing attack. *Computer*, 29(3):95–97, March 1996. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Ellison:1999:PSK

[EHMS99] C. Ellison, C. Hall, R. Milbert, and B. Schneier. Protecting secret keys with personal entropy. *Future Generation Computer Systems*, ??(??):??, ???? 1999. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). To appear.

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.

Ergun:1999:NLC

[EKK99] Funda Ergun, Joe Kilian, and Ravi Kumar. A note on the limits of collusion-resistant watermarks. *Lecture Notes in Computer Science*, 1592: 140–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920140.htm; http://link.springer-ny.com/link/service/series/0558/papers/1592/15920140.pdf.

Estrella:1999:DED

[EKLM99] F. Estrella, Z. Kovacs, J.-M. Le Goff, and R. McClatchey. The design of an engineering data warehouse based on meta-object structures. *Lecture Notes in Computer Science*, 1552: 145–156, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Eigenthaler:1984:CGA

[EKMN84] G. Eigenthaler, H. K. Kaiser, W. B. Müller, and W. Nöbauer., editors. *Contributions to general algebra, 3. Proceedings of the Vienna conference held in Vienna, June 21–24, 1984*. Hölder-Pichler-Tempsky, Vienna, Austria, 1984. ISBN 3-209-00591-5, 3-519-02762-3. LCCN ????

Evans:1974:UAS

[EKW74] Arthur Evans, Jr., William Kantrowitz, and Edwin Weiss. A user authentication scheme not requiring secrecy in the computer. *Communications of the Association for Computing Machinery*, 17(8): 437–442, August 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

EFF:1998:CSE

[Ele98] Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. 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, July 1998. ISBN 1-56592-520-3. 272 pp. LCCN QA76.9.A25 C783. US$29.95. URL http://www.eff.org/descracker/; http://www.sunworld.com/swol-07-1998/swol-07-if.html?072098a#2.

EPIC:1999:CLI

[Ele99] Electronic Privacy Information Center. *Cryptography and liberty 1999: an international survey of encryption policy*. Electronic

Privacy Information Center, Washington, DC, USA, 1999. ISBN 1-893044-03-3. 129 pp. LCCN K564.C6 C78 1999. URL http://www.epic.org/crypto/.

ElGamal:1985:PKCa

[ElG85a] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31(4):469–472, 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

ElGamal:1985:PKCb

[ElG85b] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Blakley and Chaum [BC85], pages 10–18. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=10. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

ElGamal:1985:STA

[ElG85c] Taher ElGamal. A subexponential-time algorithm for computing discrete logarithms over GF(p^2). *IEEE Transactions on Information Theory*, IT-31(4):473–481, 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Elkins:1996:RMS

[Elk96] M. Elkins. RFC 2015: MIME security with pretty good privacy (PGP), October 1996. URL ftp://ftp.internic.net/rfc/rfc2015.txt; https://www.math.utah.edu/pub/rfc/rfc2015.txt. Status: PROPOSED STANDARD.

Ellis:1997:SNS

[Ell97] J. H. Ellis. The story of non-secret encryption. Unknown, 1997.

Ellison:1998:CRN

[Ell98] C. Ellison. Cryptographic random numbers. Technical report, ????, ????, 1998. Draft P1363 Appendix E.

Ellis:1999:PPN

[Ell99] Bob Ellis. Public policy: New on-line surveys: Digital watermarking. *Computer Graphics*, 33(1):39, February 1999. CODEN CGRADI, CPGPBZ. ISSN

0097-8930 (print), 1558-4569 (electronic).

Elvin:1987:CWW

[Elv87] Robert Scott Elvin. A cryptanalysis of the World War II German Enigma cipher machine. Thesis (M.Sc.C.S.), University of New Brunswick, Ottawa, ON, Canada, 1987. 2 microfiches (104 fr.).

Even:1993:CCS

[EM93] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. *Lecture Notes in Computer Science*, 739:210–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Eades:1998:GDC

[EMMN98] P. Eades, J. Marks, P. Mutzel, and S. North. Graph drawing contest report. *Lecture Notes in Computer Science*, 1547:423–435, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ehrsam:1978:CKM

[EMMT78] William F. Ehrsam, Stephen M. Matyas, Carl H. Meyer, and Walter L. Tuchman. A cryptographic key management scheme for implementing the Data Encryption Standard. *IBM Systems Journal*, 17(2): 106–125, 1978. CODEN IBMSA7. ISSN 0018-8670.

Ezawa:1998:ATS

[EN98] K. J. Ezawa and G. Napiorkowski. Assessment of threats for smart card based electronic cash. *Lecture Notes in Computer Science*, 1465:58–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Endler:1997:PSU

[End97] David Endler. PGP: a simple usage guide. *Sys Admin: The Journal for UNIX Systems Administrators*, 6(8):21, 22, 24, 25, 27–29, 31, 32, August 1997. CODEN SYADE7. ISSN 1061-2688. URL `http://www.samag.com/archive/608art.html`.

English:1995:EEP

[Eng95] Erin English. Exportable encryption policy found 'unacceptable'. *Network Security*, 1995(12):7, December 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/1353485896897698`.

Enge:1999:ECT

[Eng99] Andreas Enge. *Elliptic curves and their applications to cryptography: an introduction*. Kluwer

Academic Publishers, Dordrecht, The Netherlands, 1999. ISBN 0-7923-8589-6. xvi + 164 pp. LCCN QA76.9.A25 E544 1999.

Ezawa:1999:AEC

[ENK99] K. J. Ezawa, G. Napiorkowski, and M. Kossarski. Assessment of effectiveness of counterfeit transaction detection systems for smart card based electronic cash. In Franklin [Fra99], pages 72–85. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Eng:1995:SDE

[EO95a] T. Eng and T. Okamoto. Single-term divisible electronic coins. *Lecture Notes in Computer Science*, 950: 306–319, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Eng:1995:STD

[EO95b] Tony Eng and Tatsuaki Okamoto. Single-term divisible electronic coins. *Lecture Notes in Computer Science*, 950:306–319, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500306.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500306.pdf.

Ephron:1998:SC

[Eph98] Henry D. Ephron. S.I.S./CB. In Deavours et al. [DKK+98], pages 241–267. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Etzel:1999:SHF

[EPR99a] M. Etzel, S. Patel, and Z. Ramzan. Square hash: Fast message authentication via optimized universal hash functions. In Wiener [Wie99], pages 234–251. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Etzel:1999:QHA

[EPR99b] Mark Etzel, Sarvar Patel, and Zulfikar Ramzan. SQUARE HASH: Fast message authentication via optimized universal hash functions. *Lecture Notes in Computer Science*, 1666: 234–251, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660234.htm; http://link.springer-

ny.com/link/service/series/0558/papers/1666/16660234.pdf.

Eizenberg:1998:PSW

[EQ98] G. Eizenberg and J.-J. Quisquater. Panel session: Watermarking. *Lecture Notes in Computer Science*, 1485:275–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Er:1989:NAG

[Er89] M. C. Er. A new algorithm for generating binary trees using rotations. *The Computer Journal*, 32 (5):470–473, October 1989. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/470.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/471.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/472.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/473.tif.

Erdem:1986:HCO

[Erd86] Hilmi Erdem. Host cryptographic operations: a software implementation. *Computers and Security*, 5(4):344–346, December 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488690057X.

Erickson:1997:DDJ

[Eri97a] Jonathan Erickson. Dr. Dobb's Journal Excellence in Programming Awards. *Dr. Dobb's Journal of Software Tools*, 22(5):18–??, May 1997. CODEN DDJOEB. ISSN 1044-789X.

Erickson:1997:DDN

[Eri97b] Jonathan Erickson. Dr. Dobb's news and views: Linux trademark issue settled; Inslaw ruling rejected; push over?; reading signs for the blind; free speech I; free speech II; Y2K insurance. *Dr. Dobb's Journal of Software Tools*, 22 (11):16, November 1997. CODEN DDJOEB. ISSN 1044-789X. URL http://www.iplawyers.com/text/linux.htm. A patent and trademark claim dispute on the name Linux has been resolved in favor of Linus Torvalds and the Linux community. A U.S. District Court Judge has ruled that source code is protected speech under the First Amendment to the U.S. Constitution, and that the U.S. Commerce Department acted illegally in requiring academics to obtains a government license before discussing cryptographic research with scholars on the Internet.

Erickson:1999:EAS

[Eri99] Jonathan Erickson. Editorial: The art and science of cryptography. *Dr. Dobb's Journal of Software Tools*, 24(12):8, December 1999. CODEN DDJOEB. ISSN 1044-789X.

Erskine:1999:CDD

[Ers99] R. Erskine. Cipher A. Deavours, David Kahn, Louis Kruh, Greg Mellen, Brian J. Winkel (eds.), Selections from Cryptologia: History, People and Technology. *Intelligence and National Security*, 14(3):247–??, 1999. CODEN ???? ISSN 0268-4527 (print), 1743-9019 (electronic).

Emerald:1997:NPC

[ES97] J. D. Emerald and K. G. Subramanian. A note on Polly Cracker public-key cryptosystems. In *Graph theory and its applications (Tirunelveli, 1996)*, pages 63–69. Tata McGraw-Hill, New Delhi, 1997.

Effelsberg:1998:SAI

[ES98] Wolfgang Effelsberg and Brian C. Smith, editors. *Sixth ACM International Multimedia Conference, 12–16 September 1998, Bristol, England*. ACM Press, New York, NY 10036, USA, 1998. ISBN 1-58113-036-8. LCCN QA76.575.A36 1998. URL `http://www.acm.org/pubs/contents/proceedings/multimedia/290747/`. ACM order number 43398.

Escott:1999:AEC

[ESST99] Adrian E. Escott, John C. Sager, Alexander P. L. Selkirk, and Dimitrios Tsapakidis. Attacking elliptic curve cryptosystems using the parallel Pollard rho method. *CryptoBytes*, 4(2): 15–19, Winter 1999. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto4n2.pdf`.

Estell:1980:BW

[Est80] Robert G. Estell. Benchmarks and watermarks. *ACM SIGMETRICS Performance Evaluation Review*, 9(3):39–44, Fall 1980. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Ettinger:1998:SGE

[Ett98] J. Mark Ettinger. Steganalysis and game equilibria. *Lecture Notes in Computer Science*, 1525: 319–328, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http:/`

/link.springer-ny.com/link/service/series/0558/bibs/1525/15250319.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250319.pdf.

Evertse:1992:WNR

[Ev92] Jan-Hendrik Evertse and Eugène van Heyst. Which new RSA-signatures can be computed from certain given RSA-signatures? *Journal of Cryptology*, 5(1): 41–52, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Even:1985:CSW

[Eve85] Shimon Even. On the complexity of some word problems that arise in testing the security of protocols. In Apostolico and Galil [AG85], pages 299–314. ISBN 0-387-15227-X. LCCN QA164 .N35 1984.

Even:1998:FVA

[Eve98] S. Even. Four value-adding algorithms. *IEEE Spectrum*, 35(5):33–38, May 1998. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Evertse:1991:WNR

[EvH91] Jan-Hendrik Evertse and Eugène van Heyst. Which new RSA signatures can be from some given RSA signatures? (extended abstract). *Lecture Notes in Computer Science*, 473: 83–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730083.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730083.pdf.

Evertse:1993:WNR

[EvH93] Jan-Hendrik Evertse and Eugène van Heyst. Which new RSA signatures can be computed from RSA signatures, obtained in a specific interactive protocol? *Lecture Notes in Computer Science*, 658:378–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580378.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580378.pdf.

Faak:1986:SVH

[Fåk86] Viiveke Fåk. Software versus hardware encryption — is there any difference today? *Computers and Security*, 5(2): 167, June 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404886901434.

Faak:1987:CMM

[Fåk87] Viiveke Fåk. Crypto management made manageable — demands on crypto equipment design. *Computers and Security*, 6(1):36–40, February 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887901234.

Falk:1988:DST

[Fal88] Adam Falk. DBMS security through encryption. Thesis (M.S.), San Francisco State University, San Francisco, CA, USA, 1988. xii + 295 pp.

Fancher:1996:SCa

[Fan96] Carol H. Fancher. Smart cards. *Scientific American*, 275(2):40–?? (Intl. ed. 24–??), August 1996. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/0896issue/0896currentissue.html.

Fancher:1997:YPS

[Fan97] C. H. Fancher. In your pocket: smartcards. *IEEE Spectrum*, 34(2):47–53, February 1997. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Farago:1967:BSS

[Far67] Ladislas Farago. *The broken seal: the story of Operation Magic and the Pearl Harbor disaster*. Random House, New York, NY, USA, 1967. 439 pp. LCCN D742.U5 F3. See also reprint [Far69].

Farago:1969:BSS

[Far69] Ladislas Farago. *The broken seal: the story of Operation Magic and the Pearl Harbor disaster*. Mayflower, London, UK, 1969. 415 pp. LCCN D742.U5 F3. Reprint of [Far67].

Farrow:1992:HIY

[Far92] Rik Farrow. How to Improve Your System Security. *UNIX/world*, 9(4):59–??, April 1992. ISSN 0739-5922.

Farrell:1993:CCC

[Far93] P. G. Farrell, editor. *Codes and cyphers: cryptography and coding IV: proceedings of the fourth IMA Conference on Cryptography and Coding organized by the Institute of Mathematics and its Applications, held at the Royal Agricultural College, Cirencester, in December 1993*. Institute of Mathematics and its

Applications, Southend-on-Sea, UK, 1993. ISBN 0-905091-03-5. LCCN ????

Ford:1997:SEC

[FB97] 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, 1997. ISBN 0-13-476342-4. xxv + 470 pp. LCCN QA76.9.A25 F66 1997.

Fox:1997:GGU

[FBS97] B. Fox, B. Beckman, and D. Simon. GUMP: Grand unified meta-protocols recipes for simple, standards-based financial cryptography. *Lecture Notes in Computer Science*, 1318:375–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fridrich:1998:RDW

[FBS98] Jiri Fridrich, Arnold C. Baldoza, and Richard J. Simard. Robust digital watermarking based on key-dependent basis functions. *Lecture Notes in Computer Science*, 1525: 143–157, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250143.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250143.pdf`.

Fenn:1996:MDD

[FBT96] S. T. J. Fenn, M. Benaissa, and D. Taylor. GF(2^m) multiplication and division over dual basis. *IEEE Transactions on Computers*, 45 (3):319–327, March 1996. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ferland:1994:PBC

[FC94] G. Ferland and J.-Y. Chouinard. Performance of BCH codes with DES encryption in a digital mobile channel. *Lecture Notes in Computer Science*, 793: 153–172, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Firoiu:1999:LER

[FC99] L. Firoiu and P. Cohen. Learning elements of representations for redescribing robot experiences. *Lecture Notes in Computer Science*, 1642:99–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

FontdecabaBaig:1998:PNL

[FCD98] E. Fontdecaba Baig, J. M. Cela Espin, and J. C. Duersteler Lopez. On the parallelisation of non-linear optimisation algorithms for ophthalmical lens design. *Lecture Notes in Computer Science*, 1541: 142–148, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fan:1999:DFS

[FCH99] H.-K. Fan, C. Chen, and C.-M. Hong. Design of fuzzy sliding controller based on cerebellar learning model. *Lecture Notes in Computer Science*, 1611:64–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Frankel:1992:PRT

[FD92] Y. Frankel and Y. Desmedt. Parallel reliable threshold multisignature. Technical Report TR-92-04-02, Department of EE & CS, University of Wisconsin-Milwaukee, Milwaukee, WI, USA, April 1992. ?? pp.

Frankel:1993:NEH

[FDB93a] Y. Frankel, Y. Desmedt, and M. Burmester. Non-existence of homomorphic general sharing schemes for some key spaces. *Lecture Notes in Computer Science*, 740:549–557, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Frankel:1993:NHG

[FDB93b] Y. Frankel, Y. Desmedt, and M. Burmester. Non-existence of homomorphic general sharing schemes for some key spaces. In Brickell [Bri93], pages 549–557. CODEN LNCSD9. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1992. DM104.00.

Feak:1983:SIS

[Fêa83] Viiveke Fêak, editor. *Security, IFIP/Sec'83: proceedings of the First Security Conference, Stockholm, Sweden, 16–19 May 1983*. North-Holland, Amsterdam, The Netherlands, 1983. ISBN 0-444-86669-8 (Elsevier). LCCN QA76.9.A25 S4 1983.

Feistel:1970:CCD

[Fei70] Horst Feistel. Cryptographic coding for data-bank privacy. Research Report RC-2827, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, March 18, 1970.

Feistel:1973:CCP

[Fei73] Horst Feistel. Cryptography and computer privacy. *Scientific American*, 228(5): 15–23, May 1973. CODEN SCAMAC. ISSN 0036-8733

(print), 1946-7087 (electronic).

Feistel:1974:BCC

[Fei74] Horst Feistel. Block cipher cryptographic system. U.S. Patent No. 3,798,359., March 19, 1974.

Feigenbaum:1991:ACC

[Fei91] Joan Feigenbaum, editor. *Advances in cryptology — CRYPTO '91: proceedings*, volume 576 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. CODEN LNCSD9. ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1991. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0576.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=576`. Conference held Aug. 11–15, 1991, at the University of California, Santa Barbara.

Feit:1993:TIA

[Fei93] Sidnie Feit. *TCP/IP: Architecture, Protocols and Implementation*. McGraw-Hill, New York, NY, USA, 1993. ISBN 0-07-020346-6. xxiii + 466 pp. LCCN TK5105.5 .F423 1993. US$44.95. Covers protocols plus additional services and products: NFS NIS, BIND, ARP, RIP, KERBEROS, SNMP, etc. Discusses hoe to invoke network services, plan name/address structure, troubleshoot, connect via bridges and routers.

Feit:1996:TIA

[Fei96] Sidnie Feit. *TCP/IP: Architecture, Protocols and Implementation*. McGraw-Hill, New York, NY, USA, second edition, 1996. ISBN 0-07-021389-5. ?? pp. LCCN TK5105.585 .F45 1996. Covers protocols plus additional services and products: NFS NIS, BIND, ARP, RIP, KERBEROS, SNMP, etc. Discusses hoe to invoke network services, plan name/address structure, troubleshoot, connect via bridges and routers.

Feigenbaum:1998:C

[Fei98] J. Feigenbaum. Crypto '91. *Lecture Notes in Computer Science*, 1440: 135–140, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Feige:1999:NSP

[Fei99] U. Feige. Noncryptographic selection protocols. In IEEE [IEE99a], pages 142–152. CODEN ASF-

PDV. ISBN 0-7695-0409-4 (softbound), 0-7803-5955-0 (casebound), 0-7695-0411-6 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1999. IEEE Catalog Number 99CB37039.

Feldman:1987:PSN

[Fel87] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In IEEE [IEE87a], pages 427–437. ISBN 0-8186-0807-2, 0-8186-4807-4 (fiche), 0-8186-8807-6 (case). LCCN QA 76 S979 1987.

Ferris:1987:WBC

[Fer87] John Ferris. Whitehall's Black Chamber: British cryptology and the Government Code and Cypher School, 1919–29. *Intelligence and National Security*, 2(1):54–??, 1987. ISSN 0268-4527 (print), 1743-9019 (electronic).

Ferguson:1998:UBD

[Fer98] N. Ferguson. Upper bounds on differential characteristics in Twofish. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, August 17, 1998. URL `http://www.counterpane.com/twofish-differential.html`.

Ferguson:1999:IDT

[Fer99a] N. Ferguson. Impossible differentials in Twofish. Twofish technical report 5, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, October 5, 1999. ???? pp. URL `http://www.counterpane.com/twofish-impossible.html`.

Fernandes:1999:ECC

[Fer99b] Andrew D. Fernandes. Elliptic-curve cryptography. *Dr. Dobb's Journal of Software Tools*, 24(12):56, 58, 60–63, December 1999. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ftp/1999/1999_12/ellip.zip`.

Feynman:1982:SPC

[Fey82] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6–7):467–488, 1982. CODEN IJTPBM. ISSN 0020-7748. Physics of computation, Part II (Dedham, Mass., 1981).

Friedman:1957:SCE

[FF57] William F. (William Frederick) Friedman and Elizebeth S. (Elizebeth Smith) Friedman. *The Shakespearean Ciphers Examined: an analysis of cryptographic systems used as evidence* *that some author other than William Shakespeare wrote the plays commonly attributed to him*. Cambridge University Press, New York, NY, USA, 1957. 4 + vii–xvi + 1 + 302 + 1 pp. LCCN PR2937 .F7.

Friedman:1955:CLS

[FFW55] William F. (William Frederick) Friedman, Elizebeth Friedman, and Louis B. (Louis Booker) Wright. *The cryptologist looks at Shakespeare*. ????, ????, 1955. ???? pp. LCCN ???? Original typescript, awarded Folger literary prize, 1955.

Feghhi:1999:DCA

[FFW99] Jalal Feghhi, Jalil Feghhi, and Peter Williams. *Digital certificates: applied Internet security*. Addison-Wesley, Reading, MA, USA, 1999. ISBN 0-201-30980-7. xxvi + 453 pp. LCCN TK5105.875.I57F44 1999. US$44.95.

Fung:1998:PAE

[FG98] W. W. Fung and J. W. Gray. Protection against EEPROM modification attacks. *Lecture Notes in Computer Science*, 1438: 250–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fuchsberger:1996:PCS

[FGLP96a] A. Fuchsberger, D. Gollmann, P. Lothian, and K. G. Paterson. Public-key cryptography on smart cards. *Lecture Notes in Computer Science*, 1029: 250–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fuchsberger:1996:PKC

[FGLP96b] A. Fuchsberger, D. Gollmann, P. Lothian, and K. G. Paterson. Public-key cryptography on smart cards. *Lecture Notes in Computer Science*, 1029: 250–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Frankel:1997:ORP

[FGMY97a] Y. Frankel, P. Gemmell, P. D. MacKenzie, and Moti Yung. Optimal resilience proactive public-key cryptosystems. In IEEE [IEE97f], pages 384–393. CODEN ASFPDV. ISBN 0-8186-8197-7 (paperback), 0-8186-8198-5 (casebound), 0-8186-8199-3 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 .S92 1997. IEEE catalog number 97CB36150. IEEE Computer Society Press order number PR08197.

Frankel:1997:PR

[FGMY97b] Yair Frankel, Peter Gemmell, Philip D. MacKenzie, and Moti Yung. Proactive RSA. In Kaliski [Kal97c], pages 440–?? CODEN LNCSD9. ISBN 3-540-63384-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1997. URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940440.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940440.pdf; http://www.cs.sandia.gov/~psgemme/crypto/rpro.html. To appear.

Feigenbaum:1992:CPM

[FGR92] Joan Feigenbaum, Eric Grosse, and James A. Reeds. Cryptographic protection of membership lists. *Newsletter of the International Association for Cryptologic Research*, 9(1):16–20, 1992. URL ftp://cm.bell-labs.com/cm/cs/doc/91/4-12.ps.Z.

Farmer:1996:SMA

[FGS96] W. Farmer, J. Guttman, and V. Swarup. Security for mobile agents: Authentication and state appraisal. *Lecture Notes in Computer Science*, 1146:118–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Frankel:1996:WCP

[FGY96a] Y. Frankel, P. Gemmell, and M. Yung. Witness-based cryptographic program checking and robust function sharing. In ACM [ACM96b], page ?? ISBN 0-89791-785-5. LCCN QA 76.6 A13 1996.

Frankel:1996:WBC

[FGY96b] Yair Frankel, Peter Gemmell, and Moti Yung. Witness-based cryptographic program checking and robust function sharing. In ACM [ACM96b], pages 499–508. ISBN 0-89791-785-5. LCCN QA 76.6 A13 1996. URL http://www.acm.org/pubs/articles/proceedings/stoc/237814/p499-frankel/p499-frankel.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/237814/p499-frankel/.

Friedman:1974:ETR

[FH74] Theodore D. Friedman and Lance J. Hoffman. Execution time requirements for encipherment programs. *Communications of the Association for Computing Machinery*, 17(8):445–449, August 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See letter [McC75].

Franklin:1994:JEM

[FH94] Matthew Franklin and Stuart Haber. Joint encryption and message-efficient secure computation. *Lecture Notes in Computer Science*, 773:266–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730266.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730266.pdf`.

Franks:1997:REH

[FHBH+97] J. Franks, P. Hallam-Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink, and L. Stewart. RFC 2069: An extension to HTTP: Digest access authentication, January 1997. URL `ftp://ftp.internic.net/rfc/rfc2069.txt; https://www.math.utah.edu/pub/rfc/rfc2069.txt`. Status: PROPOSED STANDARD.

Fabrega:1999:SSP

[FHG99] F. Javier Thayer Fábrega, Jonathan C. Herzog, and Joshua D. Guttman. Strand spaces: proving security protocols correct. *Journal of Computer Security*, 7 (2–3):191–230, ???? 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Frederickson:1984:PRT

[FHJ+84] P. Frederickson, R. Hiromoto, T. L. Jordan, B. Smith, and T. Warnock. Pseudo-random trees in Monte Carlo. *Parallel Computing*, 1(2):175–180, December 1984. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Frieze:1988:RTI

[FHK+88] Alan M. Frieze, Johan Håstad, Ravi Kannan, Jeffrey C. Lagarias, and Adi Shamir. Reconstructing truncated integer variables satisfying linear congruences. *SIAM Journal on Computing*, 17(2):262–280, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Fitzi:1998:TCP

[FHM98] M. Fitzi, M. Hirt, and U. Maurer. Trading correctness for privacy in unconditional multi-party computation. *Lecture Notes in Computer Science*, 1462: 121–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fiat:1990:BR

[Fia90] Amos Fiat. Batch RSA. *Lecture Notes in Computer Science*, 435:175–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-

3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350175.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350175.pdf.

Fiat:1994:TT

[Fia94] A. Fiat. Tracing traitors. In Desmedt [Des94b], pages 257–270. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/034127.html.

Fiat:1997:BR

[Fia97] A. Fiat. Batch RSA. *Journal of Cryptology*, 10(2):75–88, Spring 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n2p75.html; http://link.springer.de/link/service/journals/00145/bibs/10n2p75.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n2p75.tex; http://link.springer.de/link/service/journals/00145/tocs/01002.html.

Filby:1977:TPT

[Fil77] P. William Filby. Teaching Purple to talk saved thousands. *Baltimore Sun*, ??(??):??, October 16, 1977. Review of *The Man Who Broke Purple*, by Ronald Clark.

Filby:1978:BRM

[Fil78] P. William Filby. Book review: *The Man Who Broke Purple*, by Ronald Clark, 271 pages, Little, Brown. *Cryptolog*, 5(1):13–14, January 1978. ISSN 0740-7602. URL https://archive.org/download/cryptolog_38/cryptolog_38.pdf. Reprint of [Fil77].

Filby:1995:FUB

[Fil95] P. W. Filby. Floradora and a unique break into one-time pad ciphers. *Intelligence and National Security*, 10(3):408–??, 1995. ISSN 0268-4527 (print), 1743-9019 (electronic).

FIPS:1993:APG

[FIP93a] FIPS. *Automated Password Generator*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, October 5, 1993. URL http://www.itl.nist.gov/fipspubs/fip181.htm.

FIPS:1993:SHS

[FIP93b] FIPS (Federal Information Processing Standards Publication). *Secure Hash Standard: FIPS PUB 180, May 11, 1993*. United States Government Printing Office, Washington, DC, USA, May 11 1993. ?? pp.

FIPS:1994:EES

[FIP94] FIPS. *Escrowed Encryption Standard (EES)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, February 9, 1994. URL http://www.itl.nist.gov/fipspubs/fip185.htm.

Fisher:1984:CCS

[Fis84] Warren W. Fisher. Cryptography for computer security: Making the decision. *Computers and Security*, 3(3):229–233, August 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404884900440.

Fischlin:1997:ICM

[Fis97] M. Fischlin. Incremental cryptography and memory checkers. *Lecture Notes in Computer Science*, 1233: 393–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fischlin:1998:CLP

[Fis98] M. Fischlin. Cryptographic limitations on parallelizing membership and equivalence queries with applications to random self-reductions. *Lecture Notes in Computer Science*, 1501: 72–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fitzgerald:1989:QIP

[Fit89] K. Fitzgerald. The quest for intruder-proof computer systems. *IEEE Spectrum*, 26(8):22–26, August 1989. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Franz:1998:MMA

[FJ98] E. Franz and A. Jerichow. A mix-mediated anonymity service and its payment. In Quisquater et al. [Q+98], pages 313–327. ISBN 3-540-65004-0. LCCN QA267.A1 L43 no.1485. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073415.html.

Franz:1996:CBS

[FJM+96] E. Franz, A. Jerichow, S. Möller, A. Pfitzmann, and I. Stierand. Computer based steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best.

Lecture Notes in Computer Science, 1174:7–21, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054125.html.

Federrath:1996:MMC

[FJP96] H. Federrath, A. Jerichow, and A. Pfitzmann. MIXes in mobile communication systems: Location management with privacy. In Anderson [And96c], pages 121–135. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054414.html.

Friedman:1996:AFR

[FJRS96] J. Friedman, A. Joux, Y. Roichman, and J. Stern. The action of a few random permutations on r-tuples and an application to cryptography. *Lecture Notes in Computer Science*, 1046:375–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Freeman:1997:MCN

[FJV97] Martin Freeman, Paul Jardetzky, and Harrick M. Vin, editors. *Multimedia computing and networking 1997: 10–11 February, 1997, San Jose, California*, volume 3020 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 1997. ISBN 0-8194-2431-5. LCCN TS510.S63 v.3020.

Fellows:1993:KKI

[FK93a] M. Fellows and N. Koblitz. Kid krypto (invited). *Lecture Notes in Computer Science*, 740:371–389, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fellows:1993:FPC

[FK93b] Michael R. Fellows and Neal Koblitz. Fixed-parameter complexity and cryptography. In Cohen et al. [CMM93], pages 121–131. CODEN LNCSD9. ISBN 3-540-56686-4 (Berlin), 0-387-56686-4 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .A35 1993. DM72.00. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0673.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=673.

Fellows:1994:CCG

[FK94] Michael Fellows and Neal Koblitz. Combinatorial cryptosystems galore! In

Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), volume 168 of *Contemp. Math.*, pages 51–61. Amer. Math. Soc., Providence, RI, 1994.

Franke:1999:SDM

[FK99] A. Franke and M. Kohlhase. System description: MathWeb, an agent-based communication layer for distributed automated theorem proving. *Lecture Notes in Computer Science*, 1632: 217–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Freier:1996:SPV

[FKK96] A. O. Freier, P. Karlton, and P. C. Kocher. The SSL protocol — version 3.0. Internet draft draft-freier-ssl-version3-01.txt., March 1996.

Frankel:1998:BIW

[FKMY98] Y. Frankel, D. W. Kravitz, C. T. Montgomery, and M. Yung. Beyond identity: Warranty-based digital signature transactions. *Lecture Notes in Computer Science*, 1465:241–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fumy:1993:PCK

[FL93] Walter Fumy and Matthias Leclerc. Placement of cryptographic key distribution within OSI: design alternatives and assessment. *Computer Networks and ISDN Systems*, 26(2):217–225, October 1, 1993. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/comnet/cas_sub/browse/browse.cgi?year=1993&volume=26&issue=2&aid=1184`.

Fried:1996:BHA

[FL96] Benjamin Fried and Andrew Lowry. BigDog: Hierarchical authentication, session control, and authorization for the Web. In USENIX [USE96d], pages 165–172. ISBN 1-880446-83-9. LCCN HF5004 .U74 1996. URL `http://www.usenix.org/publications/library/proceedings/ec96/index.html`.

Fiadeiro:1999:ASC

[FL99a] J. L. Fiadeiro and A. Lopes. Algebraic semantics of coordination or what is in a signature? *Lecture Notes in Computer Science*, 1548: 293–307, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fox:1999:OCS

[FL99b] B. Fox and B. LaMacchia. Online certificate status checking in financial transactions: The case for re-issuance. In Franklin [Fra99], pages 104–117. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Flowers:1983:DC

[Flo83] Thomas H. Flowers. The design of Colossus. *Annals of the History of Computing*, 5(3):239–253, July/September 1983. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1983/pdf/a3239.pdf; http://www.computer.org/annals/an1983/a3239abs.htm. Foreword by Howard Campaigne.

Feiertag:1977:PMS

[FLR77] R. J. Feiertag, K. N. Levitt, and L. Robinson. Proving multilevel security of a system design. *Operating Systems Review*, 11(5):57–65, November 1977. CODEN OSRED8. ISSN 0163-5980.

Flynn:1997:WYN

[Fly97] Jim Flynn. What you need to know about Microsoft's Authenticode. *Java Report: The Source for Java Development*, 2(2):??, February 1997. CODEN JREPFI. ISSN 1086-4660. URL http://www.sigs.com/publications/docs/java/9702/java9702.toc.html.

Friedman:1976:ZTJ

[FM76] William F. (William Frederick) Friedman and Charles Jastrow Mendelsohn. *The Zimmermann telegram of January 16, 1917, and its cryptographic background*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-009-3. 33 pp. LCCN D511 .F683 1976.

Fortune:1985:PP

[FM85] Steven Fortune and Michael Merritt. Poker protocols. In Blakley and Chaum [BC85], pages 454–464. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=454. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Feigenbaum:1991:DCC

[FM91] Joan Feigenbaum and Michael Merritt. *Distributed computing and cryptogra-*

phy: proceedings of a DIMACS Workshop, October 4–6, 1989, volume 2 of *DIMACS series in discrete mathematics and theoretical computer science*. ACM Press, New York, NY 10036, USA, 1991. ISBN 0-8218-6590-0 (AMS), 0-89791-384-1 (ACM). ISSN 1052-1798. ix + 262 pp. LCCN QA76.9.D5 D43 1989. The DIMACS Workshop in Distributed Computing and Cryptography.

Faihe:1998:ADR

[FM98a] Y. Faihe and J.-P. Mueller. Analysis and design of robot's behavior: Towards a methodology. *Lecture Notes in Computer Science*, 1545:46–61, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Feustel:1998:DUI

[FM98b] Edward A. Feustel and Terry Mayfield. The DGSA: unmet information security challenges for operating system designers. *Operating Systems Review*, 32(1):3–22, January 1998. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Fairfield:1985:LRN

[FMC85] R. C. Fairfield, R. L. Mortenson, and K. B. Coulthart. An LSI random number generator (RNG). In Blakley and Chaum [BC85], pages 203–230. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=203. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Fagundes:1999:EGA

[FMM99] L. G. Fagundes, R. F. Mello, and C. E. Mdron. An environment for generating applications involving remote manipulation of parallel machines. *Lecture Notes in Computer Science*, 1586: 395–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fairfield:1985:LDE

[FMP85] R. C. Fairfield, A. Matusevich, and J. Plany. An LSI Digital Encryption Processor (DEP). In Blakley and Chaum [BC85], pages 115–143. CODEN LNCSD9.

ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=115`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Frey:1999:TPD

[FMR99] Gerhard Frey, Michael Müller, and Hans-Georg Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Transactions on Information Theory*, 45(5):1717–1719, 1999. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Frankel:1998:RED

[FMY98] Yair Frankel, Philip D. MacKenzie, and Moti Yung. Robust efficient distributed RSA-key generation. In ACM [ACM98b], pages 663–672. ISBN 0-89791-962-9. LCCN QA75.5 .A14 1998. URL `http://www.acm.org/pubs/articles/proceedings/stoc/276698/p663-frankel/p663-frankel.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/276698/p663-frankel/`. ACM order number 508980.

Fiat:1994:BE

[FN94] Amos Fiat and Moni Naor. Broadcast encryption. *Lecture Notes in Computer Science*, 773:480–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730480.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730480.pdf`.

Feistel:1975:SCT

[FNS75] H. Feistel, W. A. Notz, and J. L. Smith. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE*, 63(??):1545–1534, 1975. CODEN IEEPAD. ISSN 0018-9219 (print), 1558-2256 (electronic). URL `https://ieeexplore.ieee.org/document/1451934`.

Fiat:1992:NH

[FNSS92] Amos Fiat, Moni Naor, Jeanette P. Schmidt, and Alan Siegel. Nonoblivious hashing. *Journal of the Association for Computing Machinery*, 39(4):764–

782, October 1992. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/146591.html.

Flajolet:1989:RMS

[FO89] Philippe Flajolet and Andrew M. Odlyzko. Random mapping statistics. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *EUROCRYPT 1989: Advances in Cryptology — EUROCRYPT '89: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, volume 434 of *Lecture Notes in Computer Science*, pages 329–354. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989.

Flajolet:1990:RMS

[FO90] P. Flajolet and A. M. Odlyzko. Random mapping statistics. *Lecture Notes in Computer Science*, 434:329–354, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.research.att.com/~amo/doc/arch/random.mappings.pdf; http://www.research.att.com/~amo/doc/arch/random.mappings.ps; http://www.research.att.com/~amo/doc/arch/random.mappings.tex.

Fujisaki:1997:PEC

[FO97] E. Fujisaki and T. Okamoto. Practical escrow cash system. *Lecture Notes in Computer Science*, 1189:33–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fujisaki:1998:PPS

[FO98] E. Fujisaki and T. Okamoto. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. *Lecture Notes in Computer Science*, 1403:32–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fujisaki:1999:HES

[FO99a] Eiichiro Fujisaki and Tatsuaki Okamoto. How to enhance the security of public-key encryption at minimum cost. *Lecture Notes in Computer Science*, 1560:53–68, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1560/15600053.htm; http://link.springer-ny.com/link/service/series/0558/papers/1560/15600053.pdf.

Fujisaki:1999:SIA

[FO99b] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Wiener [Wie99], pages 537–554. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660537.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660537.pdf.

Folmsbee:1999:AJT

[Fol99] Alan Folmsbee. AES Java technology comparisons. In National Institute of Standards and Technology [Nat99b], page 28. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/Folmsbee.pdf. Only the slides for the conference talk are available.

Fujioka:1991:EED

[FOM91] Atsushi Fujioka, Tatsuaki Okamoto, and Shoji Miyaguchi. ESIGN: An efficient digital signature implementation for smart cards. *Lecture Notes in Computer Science*, 547:446–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470446.htm; http://link.springer-ny.com/link/service/series/0558/papers/0547/05470446.pdf.

Fujioka:1991:IBS

[FOO91] A. Fujioka, T. Okamoto, and K. Ohta. Interactive bi-proof systems and undeniable signature schemes. *Lecture Notes in Computer Science*, 547:243–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fujioka:1993:PSV

[FOO93] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. *Lecture Notes in Computer Science*, 718:244–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Forte:1999:BUT

[For99a] Dario Forte. Biometrics: Untruths and the truth. *;login: the USENIX Association newsletter*, 24(2): ??, April 1999. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/1999-4/biometrics.html.

Forte:1999:FAE

[For99b] Dario Forte. The future of the Advanced Encryption Standard. *Network Security*, 1999(6):10–13, June 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800800161.

Foster:1982:CM

[Fos82] Caxton C. Foster. *Cryptanalysis for microcomputers*. Hayden Book Co., Rochelle Park, NJ, USA, 1982. ISBN 0-8104-5174-3 (paperback). 333 pp. LCCN Z103.F67 1982. US$14.95.

Fox:1998:DTC

[Fox98] B. Fox. Digital TV comes down to Earth. *IEEE Spectrum*, 35(10):23–29, October 1998. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Fox:1999:NTg

[Fox99] Robert Fox. News track. *Communications of the Association for Computing Machinery*, 42(7):9–10, July 1999. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org:80/pubs/citations/journals/cacm/1999-42-7/p9-fox/.

Finocchiaro:1999:CDP

[FP99] D. V. Finocchiaro and M. Pellegrini. On computing the diameter of a point set in high dimensional Euclidean space. *Lecture Notes in Computer Science*, 1643: 366–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Frey:1994:RCD

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, April 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Ferreira:1995:PAI

[FR95a] Afonso Ferreira and Jose Rolim, editors. *Parallel algorithms for irregularly structured problems: second international workshop, IRREGULAR 95, Lyon, France, September, 4–6, 1995: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-60321-2. LCCN QA76.642.I59 1995.

Franklin:1995:LPF

[FR95b] M. Franklin and M. Reiter. A linear protocol failure for RSA with exponent three. In *????*, page ?? ????, ????, 1995. Presented at the Rump Session of Crypto '95, Santa Barbara, CA.

Franklin:1995:VSS

[FR95c] M. K. Franklin and M. K. Reiter. Verifiable signature sharing. *Lecture Notes in Computer Science*, 921: 50–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Funk:1995:CBS

[FR95d] P. J. Funk and D. Robertson. Case-based support for the design of dynamic system requirements. *Lecture Notes in Computer Science*, 984:211–222, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Franksen:1984:MBS

[Fra84] Ole Immanuel Franksen. *Mr. Babbage's secret: the tale of a cypher and APL*. Strandberg, Birkerod, Denmark, 1984. ISBN 87-87200-86-4. 319 pp. LCCN Z103.B2 F72 1984.

Franklin:1985:MID

[Fra85a] Matthew Keith Franklin. Mathematical investigations of the Data Encryption Standard. Thesis (M.A. in Mathematics), Department of Mathematics, University of California, Berkeley, Berkeley, CA, USA, May 1985. 36 pp.

Franksen:1985:MBS

[Fra85b] Ole Immanuel Franksen. *Mr. Babbage's secret: the tale of a cypher and APL*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1985. ISBN 0-13-604729-7. 319 pp. LCCN Z103.B2 F721 1985.

Franksen:1986:SHM

[Fra86] O. I. Franksen. The secret hobby of Mr. Babbage. *Systems Anal. Modelling Simulation*, 3(2):183–194, 1986. ISSN 0232-9298.

Frankel:1989:TIC

[Fra89] Yair Frankel. Two issues in cryptology: algebraic analysis of DES and a shared public key system. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1989. ix + 32 pp.

Frankel:1990:PPL

[Fra90] Y. Frankel. A practical protocol for large group oriented networks. In Quisquater and Vandewalle [QV90], pages 56–61. CODEN LNCSD9. ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1989; QA267.A1 L43 no.434. DM98.00.

Francis:1992:PSG

[Fra92] B. Francis. PC security grows up. *Datamation*, 38 (22):61–62, 64, November 1992. CODEN DTMNAT. ISSN 0011-6963.

Franksen:1993:BCM

[Fra93] Ole Immanuel Franksen. Babbage and cryptography. Or, the mystery of Admiral Beaufort's cipher. *Mathematics and Computers in Simulation*, 35(4):327–367, October 1993. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037847549390063Z`.

Franklin:1999:FCT

[Fra99] Matthew Franklin, editor. *Financial cryptography: Third International Conference, FC '99, Anguilla, British West Indies, February 22–25, 1999: proceedings*, volume 1648 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Freund:1994:KED

[Fre94] Lois A. Freund. The key escrow debate: issues and answers. Thesis (M. A.), Barry University, Miami Shores, FL, USA, 1994. 100 pp.

Friedman:1935:ICA

[Fri35a] William F. (William Frederick) Friedman. *The index of coincidence and its applications in cryptanalysis: technical paper*. United States Government Printing Office, Washington, DC, USA, 1935. 87 + 3 pp.

Friedman:1935:MCP

[Fri35b] William F. (William Frederick) Friedman. *Military cryptanalysis. Part 1, monoalphabetic substitution systems*. Number 30 in Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1935. ISBN 0-89412-044-1. 149 pp. LCCN Z103.5.F77 1992. Four volumes.

Friedman:1935:PIS

[Fri35c] William F. (William Frederick) Friedman. *The principles of indirect symmetry of position in secondary alphabets and their application in the solution of polyalphabetic substitution ciphers: technical paper*. United States Government Printing Office, Washington, DC, USA, 1935. ???? pp.

Friedman:1939:CAC

[Fri39a] William F. (William Frederick) Friedman. *The cryptanalyst accepts a challenge.*

War Department, Office of the Chief Signal Officer, Washington, DC, USA, 1939. 24–36 pp. LCCN ????

Friedman:1939:MC

[Fri39b] William F. (William Frederick) Friedman. *Military cryptanalysis*. New York Public Library, New York, NY, USA, 1939. 1 microfilm reel.

Friedman:1941:MCP

[Fri41] William F. (William Frederick) Friedman. *Military cryptanalysis. Part IV, Transposition and fractionating systems*. Cryptographic series; 61. Aegean Park Press, Laguna Hills, CA, USA, 1941. ISBN 0-89412-198-7 (paperback), 0-89412-199-5 (library bound). 189 pp. LCCN Z103.5.F77 1992.

Friedman:1942:MC

[Fri42] William F. (William Frederick) Friedman. *Military cryptanalysis*. United States Government Printing Office, Washington, DC, USA, third edition, 1942. various pp.

Friedman:1956:CCC

[Fri56] William F. (William Frederick) Friedman. *Codes and ciphers (cryptology)*. Encyclopaedia Britannica, Chicago, IL, USA, 1956. 8 pp.

Friedman:1963:SLC

[Fri63] William F. (William Frederick) Friedman. *Six lectures on cryptology*. ????, ????, 1963. iii + 182 pp.

Friedman:1976:AMC

[Fri76a] William F. (William Frederick) Friedman. *Advanced military cryptography*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-011-5. 113 pp. LCCN ???? Continuation of Elementary military cryptography, Aegean Park Press, 1976.

Friedman:1976:CEC

[Fri76b] William F. (William Frederick) Friedman. *The classic elements of cryptanalysis: with new added problems for the solver*, volume 3. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-002-6. ???? pp.

Friedman:1976:CCA

[Fri76c] William F. (William Frederick) Friedman. *Cryptography and cryptanalysis articles*, volume 5–6 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1976. ?? pp. LCCN Z103 .C79 1976.

Friedman:1976:EC

[Fri76d] William F. (William Frederick) Friedman. *Elements* *of cryptanalysis*, volume 3 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1976. 172 pp. LCCN ????

Friedman:1976:EMC

[Fri76e] William Frederick Friedman. *Elementary military cryptography*. A Cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-010-7. 86 pp. LCCN Z104 .F8740 1976. On cover: Formerly Special text no. 165 (1935).

Friedman:1987:ICA

[Fri87] William F. (William Frederick) Friedman. *The index of coincidence and its applications in cryptanalysis*, volume 49 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1987. ISBN 0-89412-137-5 (soft cover), 0-89412-138-3 (library bound). 95 pp. LCCN ????

Friedman:1992:MC

[Fri92a] William F. (William Frederick) Friedman. *Military cryptanalysis*. Number 30, 40, 60-61 in A cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1992. ISBN 0-89412-044-1 (pt. 1), 0-89412-064-6 (pt. 2), 0-89412-196-0 (pt. 3), 0-89412-198-7 (soft: pt. 4). LCCN Z103.5.F77 1992.

Friedman:1992:MCP

[Fri92b] William F. (William Frederick) Friedman. *Military cryptanalysis. Part III, Simpler varieties of aperiodic substitution systems*, volume 60 of *Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1992. ISBN 0-89412-196-0. 189 pp. LCCN Z103.5.F77 1992.

Friedmann:1993:TDC

[Fri93] G. L. Friedmann. The trustworthy digital camera: Restoring credibility to the photographic image. *IEEE Transactions on Consumer Electronics*, 39(4):905–910, November 1993. CODEN ITCEDA. ISSN 0098-3063. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/043125.html`.

Friedman:1996:SLC

[Fri96] William F. (William Frederick) Friedman. *Six lectures concerning cryptography and cryptanalysis*, volume 67 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1996. ISBN 0-89412-246-0 (paperback). 251 pp. LCCN Z103.F75 1990z.

Froomkin:1996:ICP

[Fro96] A. Michael Froomkin. It came from planet clipper: the battle over cryptographic key "escrow". Technical report, University of Chicago Law School, Chicago, IL, USA, 1996. 15–75 pp. Published in University of Chicago legal forum. Vol. 1996.

Froomkin:1997:DST

[Fro97] A. M. Froomkin. Digital signatures today. *Lecture Notes in Computer Science*, 1318:287–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fiat:1987:HPY

[FS87] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Odlyzko [Odl87b], pages 181–187. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Ferguson:1997:CA

[FS97a] N. Ferguson and B. Schneier. Cryptanalysis of Akelarre. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, August 1997. URL http://www.counterpane.com/akelarre.html. Fourth Annual Workshop on Selected Areas in Cryptography, August 1997, pp. 201–212.

Fischlin:1997:SSP

[FS97b] Roger Fischlin and Claus P. Schnorr. Stronger security proofs for RSA and Rabin bits. *Lecture Notes in Computer Science*, 1233: 267–279, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330267.htm; http://link.springer-ny.com/link/service/series/0558/papers/1233/12330267.pdf.

Forsyth:1993:ACS

[FSN93] W. S. Forsyth and R. Safavi-Naini. Automated cryptanalysis of substitution ciphers. *Austral. Comput. Sci. Comm.*, 15(1, part A): 153–161, 1993. ISSN 0157-3055.

Figueroa:1994:FCB

[FSS94] Raúl Figueroa, Pablo M. Salzberg, and Peter Jau-Shyong Shiue. A family of cryptosystems based on combinatorial properties of finite geometries. In *Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993)*, volume 168 of *Contemp. Math.*, pages 63–67. Amer. Math. Soc., Providence, RI, 1994.

Federrath:1995:SVA

[FT95] H. Federrath and J. Thees. Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern (German) [Protection of confidentiality of location of ????]. *Datenschutz und Datensicherheit*, ??(??): 338–348, June 1995. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1008.html.

Fiat:1999:DTT

[FT99a] A. Fiat and T. Tassa. Dynamic traitor tracing. In Wiener [Wie99], pages 354–371. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Frankel:1999:SID

[FT99b] Mark Frankel and Al Teich. Special issue devoted to anonymous communication on the Internet. *The Information Society*, 15(2): ??, 1999. CODEN INSCD8. ISSN 0197-2243. URL http://www.slis.indiana.edu/TIS/editor_in_chief_letters/eic152.html; http://www.slis.indiana.edu/TIS/tables_of_contents/toc.html.

Fuchs:1999:BDM

[Fuc99] H. Fuchs. Beyond the desktop metaphor: Toward more effective display, interaction, and telecollaboration in the office of the future via a multitude of sensors and displays (invited paper). *Lecture Notes in Computer Science*, 1554: 30–43, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fumy:1993:LAN

[Fum93] W. Fumy. (local area) network security. *Lecture Notes in Computer Science*, 741: 211–226, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fumy:1997:ACE

[Fum97] Walter Fumy, editor. *Advances in cryptology — EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11–15, 1997: proceedings*, volume 1233 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-

62975-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1997. Sponsored by the International Association for Cryptologic Research (IACR).

Fumy:1998:E

[Fum98a] W. Fumy. Eurocrypt '97. *Lecture Notes in Computer Science*, 1440: 215–222, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fumy:1998:ISP

[Fum98b] W. Fumy. Internet security protocols. *Lecture Notes in Computer Science*, 1528: 186–208, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fumy:1998:KMT

[Fum98c] W. Fumy. Key management techniques. *Lecture Notes in Computer Science*, 1528: 142–162, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Funk:1978:DUS

[Fun78] Mark Robert Funk. A digital ultrasound system for data collection, imaging, and tissue signature analysis. Thesis (M.S.), Department of Electrical Engineering, Michigan State University, East Lansing, MI 48824, USA, 1978. vii + 141 pp.

Funny:1993:KM

[Fun93] W. Funny. Key management. *Lecture Notes in Computer Science*, 741: 132–150, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Futrelle:1973:BTM

[Fut73] Jacques Futrelle. *Best "Thinking Machine" detective stories*. Dover Publications, Inc., New York, NY, USA, 1973. ISBN 0-486-20537-1. ix + 241 pp. LCCN PS3511.U98 B4.

Feldman:1999:HSH

[FVEA99] M. Feldman, R. Vaidyanathan, and A. El-Amawy. High speed, high capacity bused interconnects using optical slab waveguides. *Lecture Notes in Computer Science*, 1586:924–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fernandez:1987:ACA

[FVTS87] C. Fernández, A. Vaquero, J. M. Troya, and J. M. Sánchez. Automating the computation of authenticators for interbank telex messages. *Computers and Security*, 6(5):396–402, October 1987. CODEN

CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900125.

Fischer:1991:MSK

[FW91] Michael J. Fischer and Rebecca N. Wright. Multiparty secret key exchange using a random deal of cards (extended abstract). *Lecture Notes in Computer Science*, 576: 141–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760141.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760141.pdf.

Frankel:1995:CIL

[FY95a] Yair Frankel and Moti Yung. Cryptanalysis of the immunized LL public key systems. *Lecture Notes in Computer Science*, 963:287–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630287.htm; http://link.springer-ny.com/link/service/series/0558/papers/0963/09630287.pdf.

Frankel:1995:EES

[FY95b] Yair Frankel and Moti Yung. Escrow encryption systems visited: Attacks, analysis and designs. *Lecture Notes in Computer Science*, 963:222–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630222.htm; http://link.springer-ny.com/link/service/series/0558/papers/0963/09630222.pdf.

Franklin:1995:BWS

[FY95c] M. Franklin and M. Yung. The blinding of weak signatures. *Lecture Notes in Computer Science*, 950: 67–76, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Frankel:1997:CEE

[FY97] Yair Frankel and Moti Yung. On characterizations of escrow encryption schemes. *Lecture Notes in Computer Science*, 1256: 705–715, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Frankel:1998:DPK

[FY98a] Yair Frankel and Moti Yung. Distributed public key cryptosystems. *Lecture Notes in Computer Science*, 1431:1–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1431/14310001.pdf.

Frankel:1998:RMU

[FY98b] Yair Frankel and Moti Yung. Risk management using threshold RSA cryptosystems. *;login: the USENIX Association newsletter*, 23(3):??, May 1998. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/1998-5/frankel.html. Special issue on security.

Frankel:1999:CRA

[FY99] Y. Frankel and M. Yung. Cryptosystems robust against "dynamic faults" meet enterprise needs for organizational "change control". In Franklin [Fra99], pages 241–252. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Frankel:1999:ASD

[FYM99] Y. Frankel, M. Yung, and P. MacKenzie. Adaptively-secure distributed public-key systems. *Lecture Notes in Computer Science*, 1643: 4–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gritzalis:1998:SIS

[GA98] Stefanos Gritzalis and George Aggelis. Security issues surrounding programming languages for mobile code: JAVA vs. Safe-Tcl. *Operating Systems Review*, 32(2):16–32, April 1998. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Gabriel:1982:VPI

[Gab82] Richard Gabriel. Verschlüsselungsabbildungen mit Pseudo-Inversen, Zufallsgeneratoren und Täfelungen. (German) [Encryption mapping with pseudoinverses, random generators and tilings]. *Kybernetika (Prague)*, 18(6):485–504, 1982. CODEN KYBNAI. ISSN 0023-5954.

Gaddy:1991:BOP

[Gad91] David W. Gaddy. Breaking into our past: Enigmas of another kind. *Cryptolog*, 18(2):33–35, 1991. ISSN 0740-7602. URL https://archive.org/download/cryptolog_121/cryptolog_121.pdf.

Gaddy:1998:CC

[Gad98] David W. Gaddy. The cylinder-cipher. In Deavours et al. [DKK+98], pages 331–338. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Gaglione:1988:ITP

[Gag88a] A. M. Gaglione. Information theory and public key cryptosystems. *Computers and Security*, 7(5): 511, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888902167.

Gaglione:1988:SCT

[Gag88b] A. M. Gaglione. Some complexity theory for cryptography. *Computers and Security*, 7(5):519, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888902714.

Gomez-Albarran:1999:MCL

[GAGCDAFC99] M. Gomez-Albarran, P. A. Gonzalez-Calero, B. Diaz-Agudo, and C. Fernandez-Conde. Modelling the CBR life cycle using description logics. *Lecture Notes in Computer Science*, 1650: 147–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gaines:1939:ECS

[Gai39] Helen Fouche Gaines. *Elementary cryptanalysis: a study of ciphers and their solution.* American Photographic Publishing Co., Boston, MA, USA, 1939. vi + 230 + 1 pp. LCCN Z104 .G3. First edition. Galland, p. 72. Inscribed by Gelett Burgess. Bound in gray cloth; stamped in red; top edges stained red. Library of the American Cryptogram Association (George C. Lamb Collection).

Gaines:1940:ECS

[Gai40] Helen Fouche Gaines. *Elementary cryptanalysis; a study of ciphers and their solution.* Chapman and Hall, Ltd., London, UK, 1940. vi + 230 + 23 pp.

Gaines:1943:ECS

[Gai43] Helen Fouche Gaines. *Elementary cryptanalysis: a study of ciphers and their solution.* American Photographic Publishing Co., Boston, MA, USA, 1943. vi + 230 + 1 pp.

Gaines:1944:CSC

[Gai44] Helen Fouche Gaines. *Cryptanalysis: a study of ciphers and their solution.*

Dover Publications, Inc., New York, NY, USA, 1944.

Gaines:1956:CSC

[Gai56] Helen Fouché Gaines. *Cryptanalysis: a study of ciphers and their solution*. Dover Publications, Inc., New York, NY, USA, 1956. ISBN 0-486-20097-3. 237 pp. LCCN Z104 .G3 1956. Formerly published under the title: Elementary cryptanalysis.

Gait:1977:VCH

[Gai77] Jason Gait. *Validating the correctness of hardware implementations of the NBS Data Encryption Standard*. U.S. National Bureau of Standards, Gaithersburg, MD, USA, November 1977. iv + 40 pp.

Gait:1978:EEP

[Gai78] Jason Gait. Easy entry: the password encryption problem. *Operating Systems Review*, 12(3):54–60, July 1978. CODEN OSRED8. ISSN 0163-5980.

Gait:1980:CST

[Gai80a] Jason Gait. Computer science and technology: maintenance testing for the Data Encryption Standard. United States. National Bureau of Standards Special publication 500-61, U.S. National Bureau of Standards, Gaithersburg, MD, USA, 1980. 25 pp.

Gait:1980:MTD

[Gai80b] Jason Gait. *Maintenance testing for the Data Encryption Standard*. U.S. National Bureau of Standards, Gaithersburg, MD, USA, August 1980. iii + 25 pp.

Gait:1980:VCH

[Gai80c] Jason Gait. *Validating the correctness of hardware implementations of the NBS Data Encryption Standard*. United States Government Printing Office, Washington, DC, USA, 1980. iv + 40 pp. US$2.25 (paperback).

Gait:1990:VCH

[Gai90] Jason Gait. *Validating the correctness of hardware implementations of the NBS Data Encryption Standard*. Number 500-20/1980 in NBS special publication. U.S. National Bureau of Standards, Gaithersburg, MD, USA, September 1990. iv + 40 pp. LCCN QC100.A1U54 no. 500-20 19.

Gaj:1989:GCM

[Gaj89] Kris Gaj. *German Cipher Machine Enigma — Methods of Breaking*. Wydawnictwa Komunikacji i Lacznosci, Warszawa, Poland, 1989. ISBN ???? ???? pp. LCCN ????

Galland:1945:HABa

[Gal45a] Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*. Northwestern University studies in the humanities no. 10. Northwestern University, Evanston, IL, USA, 1945. viii + 11 + 209 pp. LCCN Z103.A1 G3. "Works consulted and utilized" in preface.

Galland:1945:HABb

[Gal45b] Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*. Number 10 in Northwestern University humanities series; v. 10. AMS Press, New York, NY, USA, 1945. ISBN 0-404-50710-7. viii + 209 pp. LCCN Z103.A1G3 1970.

Galland:1945:HABc

[Gal45c] Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*, volume 71 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1945. ISBN 0-89412-252-5. 209 pp. LCCN ????

Galland:1970:HAB

[Gal70] Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*. Number 10 in Northwestern University studies in the humanities. AMS Press, New York, NY, USA, 1970. ISBN 0-404-50710-7. viii + 209 pp. LCCN Z103.A1 G3 1970.

Galil:1988:SIC

[Gal88] Zvi Galil, editor. *Special issue on cryptography*, volume 17(2) of *SIAM Journal on Computing*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1988. i–viii, 179–426 pp.

Galvin:1996:PKD

[Gal96] James M. Galvin. Public key distribution with secure DNS. In USENIX [USE96e], pages 161–170. ISBN 1-880446-79-0. LCCN QA76.9.A25 U83 1996. URL `http://www.usenix.org/publications/library/proceedings/sec96/galvin.html`.

Galbraith:1999:CIB

[Gal99] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1999. CODEN ???? ISSN 1461-1570. URL `http://www.lms.ac.uk/jcm/2/lms1998-010/`.

Gamble:1988:IDL

[Gam88] Robert Oscar Gamble. Investigation of discrete logarithmic encryption algorithms. Thesis (M.S.), University of South Carolina, Columbia, SC, USA, 1988. ii + 50 pp.

Ganley:1993:CCI

[Gan93] M. J. Ganley. *Cryptography and coding III*. The Institute of Mathematics and Its Applications conference series; new ser.,; 45. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1993. ISBN 0-19-853691-7. xi + 377 pp. LCCN QA268.C75 1993. "Based on the proceedings of a conference organized by the Institute of Mathematics and its Applications on cryptography and coding, held at the Royal Agricultural College, Cirencester, in December 1991".

Ganesan:1996:HUK

[Gan96a] Ravi Ganesan. How to use key escrow. *Communications of the Association for Computing Machinery*, 39 (3):33, March 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/227238.html`; `http://www.acm.org/pubs/toc/Abstracts/cacm/227238.html`.

Ganesan:1996:YSS

[Gan96b] Ravi Ganesan. The Yaksha security system. *Communications of the Association for Computing Machinery*, 39(3):55–60, March 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/227242.html`; `http://www.acm.org/pubs/toc/Abstracts/cacm/227242.html`.

Gardner:1977:MGN

[Gar77] Martin Gardner. Mathematical games: A new kind of cipher that would take millions of years to break. *Scientific American*, 237 (2):120–124, August 1977. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v237/n2/pdf/scientificamerican0877-120.pdf`.

Garlinski:1979:IEW

[Gar79] Józef Garliński. *Intercept: the Enigma war*. J. M. Dent, London, UK, 1979. ISBN 0-460-04337-4. xx + 219 + 8 pp. LCCN D810.C88 G37.

Garlinski:1980:EW

[Gar80] Józef Garliński. *The Enigma war*. Scribner, New York, NY, USA, 1980. ISBN 0-684-15866-3. xx + 219 + 8 pp. LCCN D810.S7 G32 1980. US$14.95.

Garay:1994:RMA

[Gar94] J. A. Garay. Reaching (and maintaining) agreement in the presence of mobile faults. In Tel and Vitanyi [TV94], pages 253–264. CODEN LNCSD9. ISBN 3-540-58449-8 (Berlin), 0-387-58449-8 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.D5 I597 1994.

Garfinkel:1995:PPG

[Gar95] Simson Garfinkel. *PGP: Pretty Good Privacy*. 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, 1995. ISBN 1-56592-098-8. xxxiii + 393 pp. LCCN QA76.9.A25G36 1995. US$24.95.

Gardner:1996:PTT

[Gar96a] Martin Gardner. *Penrose tiles to trapdoor ciphers*. Spectrum series. Mathematical Association of America, Washington, DC, USA, revised edition, 1996. ISBN 0-88385-521-6 (paperback). ???? pp. LCCN 9609 BOOK NOT YET IN LC. URL `http://www.loc.gov/catdir/description/cam028/96077786.html; http://www.loc.gov/catdir/toc/cam027/96077786.html`.

Garfinkel:1996:IKP

[Gar96b] S. L. Garfinkel. Internet kiosk: Public key cryptography. *Computer*, 29(6): 101–104, June 1996. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Garfinkel:1996:JSC

[Gar96c] Simson L. Garfinkel. Java security cracked: Again and again. *WebServer Magazine: For Managers of World Wide Web Sites*, 1 (2):8, July/August 1996. ISSN 1087-4232. URL `http://www.cpg.com`.

Garber:1997:NBAa

[Gar97a] Lee Garber. News briefs: Agency: Net use hasn't hurt US phone system; Apple unveils turnaround strategy; JTC rejects Java standards plan; vendors plan 300-nm wafers; battle brews over smart card encryption; countries lift Internet telephone ban; Motorola proposes satellite system; vendors agree on high-capacity disks; "wrapping" software sales; Tonga offers domain name alternative. *Computer*, 30(9):19–22, September 1997. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://neumann.computer.org/co/books/co1997/pdf/r9019.pdf`.

Garber:1997:NBB

[Gar97b] Lee Garber. News briefs: Binary version could bring VRML into the mainstream. FCC jumps into Internet fray. Java and floating-point math. Intel to design NDRAM. battle over net telephony. vendors seek fast modems. US permits export of strong encryption. E-commerce nears $1 billion. chasing the blue light. personal E-mail use will soar. *Computer*, 30(4): 25–27, April 1997. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Garber:1997:NBC

[Gar97c] Lee Garber. News briefs: Crucial compromise launches digital TV. US encryption agreement in jeopardy. warning issued about UNIX flaw. WIPO discusses cyberspace copyrights. IT issues could threaten European Monetary Union. COBOL programmers in demand again. chip alliance formed. semiconductor film grown in space. survey reveals security fears and vulnerability. taxing the Internet. *Computer*, 30(2): 18, 19, 22, February 1997. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Gardner:1997:PTT

[Gar97d] Martin Gardner. *Penrose tiles to trapdoor ciphers, and the return of Dr. Matrix*. MAA spectrum. Mathematical Association of America, Washington, DC, USA, revised edition, 1997. ISBN 0-88385-521-6 (paperback). ix + 319 pp. LCCN QA95 .G298 1997.

Garber:1998:NBM

[Gar98a] Lee Garber. News briefs; moving 3D beyond VRML; US, Microsoft will square off on September 8; satellite processor failure cuts net, pager service; US seeks encryption standard; vendors unveil Bluetooth wireless technology; the end of MS-DOS. *Computer*, 31 (7):18–21, July 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co1998/pdf/r7018.pdf`.

Garber:1998:NBS

[Gar98b] Lee Garber. News briefs: Sun gets OK to propose Java standards; domain name plan delayed; encryption battle heats up; monstor processes to debut in 1998; work begins on API for digital TV; ISO approves C++ Standard; new standard for parallel processing workstations; IBM unveils high-capacity disk technology. *Computer*, 31(1):21–24, January 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://pdf.computer.org/co/books/co1998/pdf/r1021.pdf`.

Garfinkel:1998:PPG

[Gar98c] Simson Garfinkel. *PGP: Pretty Good Privacy: sifrovani pro kazdeho*. Computer Press, Praha, Czech Republic, 1998. ISBN 80-7226-054-5 (broz.). 373 pp. LCCN ????

Gaudin:1997:VBJ

[Gau97] Sharon Gaudin. Visa boosts Java's credit line: smart cards will redefine how plastic is used. *Computerworld*, 31(31):1, 16, August 4, 1997. CODEN CMPWAB. ISSN 0010-4841.

Gilmour-Bryson:1982:CDT

[GB82] A. Gilmour-Bryson. Coding of the depositions of the Templars. In Ciampi and Martino [CM82], pages 451–467. ISBN 0-444-86413-X (set), 0-444-86414-8 (vol. 1), 0-444-86415-6 (vol. 2). LCCN K662.I4 I58. From *Computing Reviews*: "The article reports on the progress of an historical study using a computer for statistical analysis. The subject of the study is a mass of trial depositions of the Knights Templar. The purpose of the project is to find statistical regularities in the large amount of testimony and to create a model for similar studies. The Order of the Knights Templar, founded around 1100, was the first Christian military order. After the Crusades, in the early fourteenth century, 127 articles of accusation were brought against the order, including charges of idolatry, sacrilege, and sodomy. The data being studied are the responses of 900 men to each of 127 accusations. The article details the accusations and the way in which the responses are being coded. The statistical package SAS (Statistical Analysis System) will be used. Examples of the results to be sought are: tallies of guilty/innocent responses, tallies of offenses committed versus seen versus heard about, and correlations between, for example, age and other responses. Depositions that differ markedly from the average response will be identified.".

Golshani:1998:NDW

[GB98] Forouzan Golshani and Robin Baldwin. In the news: Digital-watermarking faces challenges; virtual human agents evolve; vendors urge, give SET a chance; radio on the net; media notes. *IEEE MultiMedia*, 5(3):6–9, July–September 1998. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL `http://dlib.computer.org/mu/books/mu1998/pdf/u3006.pdf`.

Geoffroy:1993:APF

[GBC93] M. Geoffroy, R. Bjones, and H. Cnudde. AXYTRANS: Physical funds transport and DES. *Lecture Notes in Computer Science*, 741: 244–256, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gong:1994:AKD

[GBL94] Li Gong, T. A. (Thomas A.) Berson, and T. Mark A. Lomas. Authentication, key distribution, and secure broadcast in computer networks using no encryption or decryption. Technical report SRI-CSL-94-08, SRI International, Computer Science Laboratory, Menlo Park, CA, USA, 1994. 13 + 4 + 10 pp.

Goethals:1980:CAL

[GC80] J.-M. Goethals and C. Couvreur. A cryptanalytic attack on the Lu-Lee public-key cryptosystem. *Philips Journal of Research*, 35(4-5):301–306, 1980. CODEN PHJRD9. ISSN 0165-5817.

Gollmann:1990:CC

[GC90] Dieter Gollmann and William G. Chambers. A cryptanalysis of $\mathrm{Step}_{k,m}$-cascades. *Lecture Notes in Computer Science*, 434: 680–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340680.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0434/04340680.pdf`.

Gilbert:1991:SAF

[GC91] Henry Gilbert and Guy Chassé. A statistical attack of the FEAL-8 cryptosystem. *Lecture Notes in Computer Science*, 537: 22–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370022.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0537/05370022.pdf`.

Gilbert:1994:CPA

[GC94] Henri Gilbert and Pascal Chauvaud. A chosen plaintext attack of the

16-round Khufu cryptosystem. In Desmedt [Des94b], pages 359–368. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390359.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390359.pdf.

Garber:1997:NBJ

[GC97] Lee Garber and David Clark. News briefs: Judge rejects US restrictions on export of encryption; Intel, HP unveil Merced chip; Java wars heat up; AOL acquires CompuServe subscribers; confusion in the DVD marketplace; 'amazing grace' heads to sea; PC firms back down on convergence; business use will drive Internet growth; company offers $1-million prize for hackers. *Computer*, 30(11):22–25, November 1997. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://pdf.computer.org/co/books/co1997/pdf/ry022.pdf.

Gershenfeld:1998:QCM

[GC98] Neil Gershenfeld and Isaac L. Chuang. Quantum computing with molecules. *Scientific American*, 278(6):66–71, June 1998. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Girault:1988:GBA

[GCC88] Marc Girault, Robert Cohen, and Mireille Campana. A generalized birthday attack. In Gunther [Gun88b], pages 129–156. CODEN LNCSD9. ISBN 0-387-50251-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.330; QA76.9.A25 E9641 1988. Sponsored by the International Association for Cryptologic Research.

Goffin:1997:LCP

[GDD+97] F. Goffin, J. F. Delaigle, C. De Vleeschouwer, B. Macq, and J. J. Quisquater. A low cost perceptive digital picture watermarking method. In Sethi and Jain [SJ97], pages 264–277. ISBN 0-8194-2433-1. LCCN TS510.S63 v.3022. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/063129.html.

Goldburg:1991:ACA

[GDS91] B. Goldburg, E. Dawson, and S. Sridharan. The automated cryptanalysis of analog speech scramblers. *Lecture Notes in Computer Science*, 547:422–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Geffe:1973:HPD

[Gef73] P. Geffe. How to protect data with ciphers that are really hard to break. *Electronics*, 46(1):99–101, 1973. ISSN 0883-4989. This cipher was later broken by [Sie85].

Gehrmann:1994:CGN

[Geh94] Christian Gehrmann. Cryptanalysis of the Gemmell and Naor multiround authentication protocol. In Desmedt [Des94b], pages 121–128. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390121.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390121.pdf.

Gehrmann:1995:SMA

[Geh95] Christian Gehrmann. Secure multiround authentication protocols. *Lecture Notes in Computer Science*, 921:158–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210158.htm; http://link.springer-ny.com/link/service/series/0558/papers/0921/09210158.pdf.

Gelb:1974:RWD

[Gel74] I. J. Gelb. Records, writing, and decipherment. *Visible Language*, VIII(4):293–318, Autumn 1974. CODEN VSLGAO. ISSN 0022-2224 (print), 2691-5529 (electronic). URL https://s3-us-west-2.amazonaws.com/visiblelanguage/pdf/V8N4_1974_E.pdf.

Gray:1998:PSC

[GEL98] James W. Gray III, Kin Fai Epsilon Ip, and King-Shan Lui. Provable security for cryptographic protocols — exact analysis and engineering applications. *Journal of Computer Security*, 6(1–2):23–52, ???? 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gemmell:1997:ITC

[Gem97] Peter S. Gemmell. An introduction to threshold cryptography. *CryptoBytes*, 2(3):7–12, Winter 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n3.pdf.

Gengler:1998:ESR

[Gen98a] Barbara Gengler. Encryption standard replaced. *Network Security*, 1998(9):5–6, September 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898800135.

Gengler:1998:INC

[Gen98b] Barbara Gengler. IBM's new cryptosystem. *Network Security*, 1998(9):5, September 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898800123.

Gengler:1999:EEL

[Gen99a] Barbara Gengler. Encryption export laws. *Network Security*, 1999(12):5–6, December 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800872451.

Gengler:1999:ELM

[Gen99b] Barbara Gengler. Encryption laws may slacken. *Network Security*, 1999(4):4, April 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899901824.

Gengler:1999:NCG

[Gen99c] Barbara Gengler. Now cryptography gets the 'open source' treatment. *Network Security*, 1999(6):6, June 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899900582.

Gersho:1982:ACR

[Ger82] Allen Gersho. *Advances in cryptography: a report on CRYPTO 81*. Santa Barbara, CA, USA, 1982. viii + 156 pp. "Sponsored by the Data and Computer Communications Committees of the IEEE Communications Society with the cooperation of the Dept. of Electrical and Computer Engineering, University of California, Santa Barbara." — Verso of t.p. "August 20, 1982." Includes bibliographies.

Gerling:1997:VKU

[Ger97] R. W. Gerling. Verschlüsselungsverfahren — Eine Kurz übersicht (German) [Coding practice: a course overview]. *Datenschutz und Datensicherheit*, 21(4):197–201, April 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/062326.html.

Gersho:1998:C

[Ger98] A. Gersho. Crypto '81. *Lecture Notes in Computer Science*, 1440:3–8, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gero:1999:NME

[Ger99a] J. S. Gero. Novel models in evolutionary designing. *Lecture Notes in Computer Science*, 1585:381–388, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gero:1999:RRA

[Ger99b] J. S. Gero. Representation and reasoning about shapes: Cognitive and computational studies in visual reasoning in design. *Lecture Notes in Computer Science*, 1661:315–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ghezzi:1993:RSS

[GFB93] C. Ghezzi, M. Felder, and C. Bellettini. Real-time systems: a survey of approaches to formal specification and verification. *Lecture Notes in Computer Science*, 717:11–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldreich:1997:EDE

[GGH97a] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Eliminating decryption errors in the Ajtai–Dwork cryptosystem. *Lecture Notes in Computer Science*, 1294:105–111, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldreich:1997:PKC

[GGH97b] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. *Lecture Notes in Computer Science*, 1294: 112–131, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940112.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940112.pdf`.

Gilbert:1998:DFC

[GGH+98] H. Gilbert, M. Girault, P. Hoogvorst, F. Noilhan, T. Pornin, G. Poupard, J. Stern, and S. Vaudenay. Decorrelated fast cipher: an AES candidate. In National Institute of Standards and Technology [Nat98], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf1/aes1conf.htm; http://www.nist.gov/aes. See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen "complete and proper" candidates.

Gabber:1999:SPC

[GGK+99] Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, and Alain Mayer. On secure and pseudonymous client-relationships with multiple servers. *ACM Transactions on Information and System Security*, 2(4):390–415, November 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org/pubs/citations/journals/tissec/1999-2-4/p390-gabber/.

Goldreich:1985:CAR

[GGM85] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. On the cryptographic applications of random functions (extended abstract). In Blakley and Chaum [BC85], pages 276–288. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=276. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Goldreich:1986:HCR

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the Association for Computing Machinery*, 33(4):792–807, October 1986. CODEN JACOAH. ISSN 0004-5411. URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/6503.html. A computational complexity measure of the randomness of functions is introduced, and, assuming the existence of one-way functions, a pseudo-random function generator is presented.

Gabber:1997:HMP

[GGMM97] E. Gabber, P. B. Gibbons, Y. Matias, and A. Mayer. How to make personalized Web browsing simple, secure, and anonymous. In

Hirschfeld [Hir97], pages 17–31. CODEN LNCSD9. ISBN 3-540-63594-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/071123.html.

Gilbert:1998:ASR

[GGOQ98] Henri Gilbert, Dipankar Gupta, Andrew Odlyzko, and Jean-Jacques Quisquater. Attacks on Shamir's 'RSA for paranoids'. *Information Processing Letters*, 68(4):197–199, November 30, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.research.att.com/~amo/doc/rsa.for.paranoids.pdf; http://www.research.att.com/~amo/doc/rsa.for.paranoids.ps; http://www.research.att.com/~amo/doc/rsa.for.paranoids.tex.

Gittler:1995:DSS

[GH95] Frederic Gittler and Anne C. Hopkins. The DCE security service. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 46(6):41–48, December 1995. CODEN HPJOAX. ISSN 0018-1153. URL http://www.hp.com/hpj/95dec/dec95_41.pdf; http://www.hp.com/hpj/toc-12-95.html.

Gehrke:1996:MPK

[GH96] Michael Gehrke and Thomas Hetschold. Management of a public key certification infrastructure — Experiences from the DeTeBerkom project BMSec. *Computer Networks and ISDN Systems*, 28(14):1901–1914, November 1, 1996. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic). URL http://www.elsevier.com/cas/tree/store/comnet/sub/1996/28/14/1647.pdf.

Gong:1999:PKC

[GH99] Guang Gong and Lein Harn. Public-key cryptosystems based on cubic finite field extensions. *IEEE Transactions on Information Theory*, 45(7):2601–2605, 1999. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Gennaro:1999:SHS

[GHR99] R. Gennaro, S. Halevi, and T. Rabin. Secure hash-and-sign signatures without the random oracle. *Lecture Notes in Computer Science*, 1592:123–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gopalakrishnan:1993:NCC

[GHS93] K. Gopalakrishnan, D. G. Hoffman, and D. R. Stinson. A note on a conjecture concerning symmetric resilient functions. *Information Processing Letters*, 47(3):139–143, September 14, 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Galil:1990:SPK

[GHY90] Zvi Galil, Stuart Haber, and Moti Yung. A secure public-key authentication scheme. *Lecture Notes in Computer Science*, 434:3–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340003.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340003.pdf`.

Gilboa:1999:CCR

[GI99] N. Gilboa and Y. Ishai. Compressing cryptographic resources. In Wiener [Wie99], pages 591–608. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Gibson:1990:SCD

[Gib90] J. K. Gibson. Some comments on Damgård's hashing principle. *Electronics Letters*, 26(15):1178–1179, July 19, 1990. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic).

Gibson:1991:EGC

[Gib91] J. Keith Gibson. Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem. *Lecture Notes in Computer Science*, 547:517–521, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470517.htm; http://link.springer-ny.com/link/service/series/0558/papers/0547/05470517.pdf`.

Gibson:1995:SDG

[Gib95] J. K. Gibson. Severely denting the Gabidulin version of the McEliece public key cryptosystem. *Designs, Codes, and Cryptography*, 6(1):37–45, 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Gibson:1996:SGP

[Gib96] Keith Gibson. The security of the Gabidulin public key cryptosystem. *Lecture Notes in Computer Science*, 1070:212–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700212.htm; http://link.springer-ny.com/link/service/series/0558/papers/1070/10700212.pdf.

Gifford:1981:CSI

[Gif81] David K. Gifford. Cryptographic sealing for information secrecy and authentication. *Operating Systems Review*, 15(5):123–124, December 1981. CODEN OSRED8. ISSN 0163-5980.

Gilder:1997:APD

[Gil97] Tyson T. Gilder. Analyzing and predicting data encryption use with the technology acceptance model. Thesis (M.S.), Department of Computer Information Systems, Colorado State University, Fort Collins, CO, USA, 1997. v + 49 pp.

Giles:1998:EFS

[Gil98] Bear Giles. Encrypted file systems. *Linux Journal*, 51:??, July 1998. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Gilboa:1999:TPR

[Gil99] Niv Gilboa. Two party RSA key generation (extended abstract). In Wiener [Wie99], pages 116–129. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660116.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660116.pdf.

Gingerich:1970:BRB

[Gin70] Owen Gingerich. Book review: *The Codebreakers. The Story of Secret Writing* by David Kahn. *Isis*, 61(3):405–406, Autumn 1970. CODEN ISISA4. ISSN 0021-1753 (print), 1545-6994 (electronic). URL http://www.jstor.org/stable/229701.

Girdansky:1971:DPC

[Gir71] M. B. Girdansky. Data privacy — cryptology and the computer at IBM Research,. *IBM Research Reports*, 7 (4):12, 1971.

Girdansky:1972:CCD

[Gir72] M. B. Girdansky. Cryptology, the computer and data privacy. *Computers and Automation*, 21(??):12–19, April 1972.

Girling:1987:CCL

[Gir87] C. G. Girling. Covert channels in LAN's. *IEEE Transactions on Software Engineering*, SE-13(2):292–296, February 1987. CO-

DEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702208.

Girault:1991:SCP

[Gir91] Marc Girault. Self-certified public keys. *Lecture Notes in Computer Science*, 547: 490–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470490.htm; http://link.springer-ny.com/link/service/series/0558/papers/0547/05470490.pdf.

Girard:1999:WSP

[Gir99] Pierre Girard. Which security policy for multiapplication Smart Cards? In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL http://www.usenix.org/publications/library/proceedings/smartcard99/girard.html.

Givierge:1925:CC

[Giv25] Marcel Givierge. *Cours de cryptographie*. Berger-Levrault, Paris, France, 1925. ix + 304 pp. LCCN Z104 .G43.

Givierge:1932:CC

[Giv32] Marcel Givierge. *Cours de cryptographie*. Berger-Levrault, Paris, France, deuxième edition, 1932. ix + 304 pp.

Givierge:1978:CC

[Giv78] Marcel Givierge. *Course in cryptography*, volume 19 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1978. ISBN 0-89412-028-X. 164 pp. English translation of [Giv32].

Garey:1979:CIG

[GJ79] Michael R. Garey and David S. Johnson. *Computers and Intractability: a Guide to the Theory of NP-Completeness*. W.H. Freeman, San Francisco, CA, USA and New York, NY, USA, 1979. ISBN 0-7167-1045-5, 0-7167-1044-7. x + 338 pp.

Gifford:1982:CSI

[GJ82] D. K. Gifford and A. K. Jones. Cryptographic sealing for information security and authentication. *Communications of the Association for Computing Machinery*, 25(4):274–286, April 1982. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Gennaro:1996:RTD

[GJKR96a] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold DSS signatures. In Maurer [Mau96b], pages 354–371. CODEN LNCSD9. ISBN 3-540-61186-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1996. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1070.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1070. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Gennaro:1996:RES

[GJKR96b] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Robust and efficient sharing of RSA functions. In Koblitz [Kob96], pages 157–172. CODEN LNCSD9. ISBN 3-540-61512-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1996. URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090157.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090157.pdf. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Gennaro:1999:SDK

[GJKR99] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. *Lecture Notes in Computer Science*, 1592:295–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Garay:1999:AFO

[GJM99a] J. A. Garay, M. Jakobsson, and P. MacKenzie. Abuse-free optimistic contract signing. *Lecture Notes in Computer Science*, 1666: 449–466, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Garay:1999:AOC

[GJM99b] J. A. Garay, M. Jakobsson, and P. MacKenzie. Abuse-free optimistic contract signing. In Wiener [Wie99], pages 449–466. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Goresky:1995:FRB

[GK95a] M. Goresky and A. Klapper. Feedback registers based on ramified extensions of the 2-adic numbers. *Lecture Notes in Computer Science*, 950:215–222, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gurses:1995:VCT

[GK95b] Metin Gürses and Atalay Karasu. Variable coefficient third order Korteweg–de Vries type of equations. *Journal of Mathematical Physics*, 36(7):3485–3491, July 1995. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.

Goldreich:1996:CZP

[GK96] O. Goldreich and H. Krawczyk. On the composition of zero-knowledge proof systems. *SIAM Journal on Computing*, 25(1):169–192, February 1996. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Glenn:1998:RNE

[GK98] R. Glenn and S. Kent. RFC 2410: The NULL encryption algorithm and its use with IPsec, November 1998. URL ftp://ftp.internic.net/rfc/rfc2410.txt; https://www.math.utah.edu/pub/rfc/rfc2410.txt. Status: PROPOSED STANDARD.

Goldschlag:1999:BCC

[GK99a] David M. Goldschlag and David W. Kravitz. Beyond cryptographic conditional access. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL http://www.usenix.org/publications/library/proceedings/smartcard99/goldschlag.html.

Goldwasser:1999:PTU

[GK99b] Shafi Goldwasser and Joe Kilian. Primality testing using elliptic curves. *Journal of the Association for Computing Machinery*, 46(4):450–472, July 1999. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL http://www.acm.org/pubs/articles/journals/jacm/1999-46-4/p450-goldwasser/p450-goldwasser.pdf; http://www.acm.org/pubs/citations/journals/jacm/1999-46-4/p450-goldwasser/.

Gennaro:1997:RBU

[GKR97] Rosario Gennaro, Hugo Krawczyk, and Tal Rabin. RSA-based undeniable signatures. *Lecture Notes in Computer Science*, 1294:132–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/

link/service/series/0558/bibs/1294/12940132.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940132.pdf.

Gotz:1997:DTC

[GKS97] Marco Götz, Kristina Kelber, and Wolfgang Schwarz. Discrete-time chaotic encryption systems. I. Statistical design approach. *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, 44(10): 963–970, 1997. CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic). Special issue on chaos synchronization, control, and applications.

Gligor:1979:OMA

[GL79] V. D. Gligor and B. G. Lindsay. Object migration and authentication. *IEEE Transactions on Software Engineering*, SE-5(6):607–611, November/December 1979. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702677.

Guillou:1982:CT

[GL82] L. C. Guillou and B. Lorig. Cryptography and tele-informatics. *Computers and Security*, 1(1):27–33, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404882900220.

Goldreich:1989:HCP

[GL89] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In ACM-TOC'89 [ACM89c], pages 25–32. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. URL http://www.acm.org/pubs/articles/proceedings/stoc/73007/p25-goldreich/p25-goldreich.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/73007/p25-goldreich/.

Gaskell:1996:ISC

[GL96] G. Gaskell and M. Looi. Integrating smart cards into authentication systems. *Lecture Notes in Computer Science*, 1029: 270–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gladman:1999:IEA

[Gla99a] Brian Gladman. Implementation experience with AES candidate algorithms. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/

encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Gladwin:1999:CCS

[Gla99b] Lee A. Gladwin. Cautious collaborators: The struggle for Anglo-American cryptanalytic co-operation, 1940–43. *Intelligence and National Security*, 14(1): 119–??, 1999. ISSN 0268-4527 (print), 1743-9019 (electronic).

Gruhl:1996:EH

[GLB96] D. Gruhl, A. Lu, and W. Bender. Echo hiding. In Anderson [And96c], pages 295–315. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054134.html.

Georgoudis:1998:TPF

[GLC98] Dianelos Georges Georgoudis, Damian Leroux, and Billy Simón Chaves. TecApro presents Frog: An AES candidate algorithms. In National Institute of Standards and Technology [Nat98], page 19. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf1/frog-slides.pdf. Only the slides for the conference talk are available.

Gleason:1957:ECP

[Gle57] Andrew M. Gleason. *Elementary course in probability*. National Security Agency, Office of Research and Development, Mathematical Research Division, Washington, DC, USA, second edition, 1957. various pp. LCCN Z104 .G53 1957. Revised by Walter F. Penney and Ronald E. Wyllys.

Gleason:1986:ECP

[Gle86] Andrew M. Gleason. *Elementary course in probability for the cryptanalyst*. Aegean Park Press, Laguna Hills, CA, USA, 1986. ISBN 0-89412-098-0. ???? pp. LCCN ????

Gleason:1987:PIC

[Gle87] Andrew M. Gleason, editor. *Proceedings of the International Congress of Mathematicians, 1986: August 3–11, 1986, Berkeley*. American Mathematical Society, Providence, RI, USA, 1987. ISBN 0-8218-0110-4. LCCN QA1 .I8 1986 v. 1-2. Two volumes.

Gonzalez:1999:RMT

[GLSM99] E. Gonzalez, H. Loaiza, A. Surez, and C. Morenoet.

Real MagiCol 98: Team description and results. *Lecture Notes in Computer Science*, 1604:440–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gallant:1999:IPP

[GLV99] Robert Gallant, Robert Lambert, and Scott Vanstone. Improving the parallelized Pollard lambda search on anomalous binary curves. *Mathematics of Computation*, 68(??): ??, ???? 1999. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). To appear.

Gamage:1999:EMA

[GLZ99] Chandana Gamage, Jussipekka Leiwo, and Yuliang Zheng. Encrypted message authentication by firewalls. *Lecture Notes in Computer Science*, 1560: 69–81, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1560/15600069.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1560/15600069.pdf`.

Goldwasser:1982:PEH

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In ACM [ACM82], pages 365–377. ISBN 0-89791-070-2. LCCN QA75.5 .A14 1982. ACM order no. 508820.

Goldwasser:1984:PE

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984. CODEN JCSSBM. ISSN 0022-0000. See also preliminary version in 14th STOC, 1982.

Goodman:1985:NTK

[GM85] R. M. F. Goodman and A. J. McAuley. A new trapdoor knapsack public key cryptosystem. *Lecture Notes in Computer Science*, 209:150–158, 1985. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Godlewski:1990:KMA

[GM90] Philippe Godlewski and Chris Mitchell. Key minimal authentication systems for unconditional secrecy. *Lecture Notes in Computer Science*, 434: 497–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340497.htm`;

http://link.springer-ny.com/link/service/series/0558/papers/0434/04340497.pdf.

Golic:1991:NCC

[GM91] Jovan Dj. Golić and Miodrag J. Mihaljević. A noisy clock-controlled shift register cryptanalysis concept based on sequence comparison approach. *Lecture Notes in Computer Science*, 473: 487–491, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Galvin:1993:RSP

[GM93a] J. Galvin and K. McCloghrie. RFC 1446: Security protocols for version 2 of the Simple Network Management Protocol (SNMPv2), April 1993. URL ftp://ftp.internic.net/rfc/rfc1446.txt; https://www.math.utah.edu/pub/rfc/rfc1446.txt. Status: HISTORIC.

Gordon:1993:MPC

[GM93b] D. M. Gordon and K. S. McCurley. Massively parallel computation of discrete logarithms. *Lecture Notes in Computer Science*, 740: 312–323, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gennaro:1995:VSS

[GM95] R. Gennaro and S. Micali. Verifiable secret sharing as secure computation. *Lecture Notes in Computer Science*, 921:168–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Girault:1997:SFR

[GM97] Marc Girault and Jean-François Misarsky. Selective forgery of RSA signatures using redundancy. *Lecture Notes in Computer Science*, 1233:495–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330495.htm; http://link.springer-ny.com/link/service/series/0558/papers/1233/12330495.pdf.

GomezdeSilvaGarza:1999:EAC

[GM99a] A. Gomez de Silva Garza and M. L. Maher. An evolutionary approach to case adaptation. *Lecture Notes in Computer Science*, 1650: 162–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Grohe:1999:DDC

[GM99b] M. Grohe and J. Mariño. Definability and descriptive complexity on databases of bounded tree-width. *Lecture Notes in Computer Science*, 1540:70–82, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Galvin:1995:RSM

[GMCF95] J. Galvin, S. Murphy, S. Crocker, and N. Freed. RFC 1847: Security multiparts for MIME: Multipart/signed and multipart/encrypted, October 1995. URL ftp://ftp.internic.net/rfc/rfc1847.txt; https://www.math.utah.edu/pub/rfc/rfc1847.txt. Status: PROPOSED STANDARD.

Griwodz:1998:PVE

[GMDS98] C. Griwodz, O. Merkel, J. Dittmann, and R. Steinmetz. Protecting VoD the easier way. In Effelsberg and Smith [ES98], pages 21–28. ISBN 1-58113-036-8. LCCN QA76.575.A36 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073127.html. ACM order number 43398.

Ghazi-Moghaddam:1994:OCH

[GMLH94] F. Ghazi-Moghaddam, I. Lambadaris, and J. F. Hayes. Overflow constraint in hybrid nodes with movable boundary scheme. *Lecture Notes in Computer Science*, 793:296–309, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldwasser:1985:PSS

[GMR85] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A “Paradoxical” solution to the signature problem. In Blakley and Chaum [BC85], page 467. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=467. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Goldwasser:1988:DSS

[GMR88] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Goldwasser:1989:KCI

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, February 1989. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Good:1945:GRT

[GMT45] I. Jack Good, Donald Michie, and Geoffrey Timms. General report on Tunny. GC&CS report HW 25/4, British National Archives, ????, 1945.

Groote:1998:CVP

[GMV98] J. F. Groote, F. Monin, and J. C. Van de Pol. Checking verifications of protocols and distributed systems by computer. *Lecture Notes in Computer Science*, 1466:629–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldreich:1987:HPM

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game — A completeness theorem for protocols with honest majority. In ACM [ACM87], pages 218–229. ISBN 0-89791-221-7. LCCN QA 76.6 A13 1987.

Goldreich:1991:PYN

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the Association for Computing Machinery*, 38(3):691–729, July 1991. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/116852.html`. They show that for a language L in NP and a string w in L, there exists a probabilistic interactive proof that efficiently demonstrates membership of x in L without conveying additional information. Previously, zero-knowledge proofs were known only for some problems that were in both NP and $co\text{-}NP$. A preliminary version of this paper appeared in *Proc. 27th Ann. IEEE Symp. on Foundations of Computer Science*, 1986, under the title “Proofs that yield nothing but their validity and a methodology of cryptographic protocol design.”.

Gemmell:1994:CIA

[GN94] Peter Gemmell and Moni Naor. Codes for interactive authentication. *Lecture Notes in Computer Sci-*

ence, 773:355–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730355.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730355.pdf.

Goettfert:1995:GLB

[GN95a] R. Goettfert and H. Niederreiter. A general lower bound for the linear complexity of the product of shift-register sequences. *Lecture Notes in Computer Science*, 950:223–229, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gray:1995:PCT

[GN95b] J. P. Gray and F. Naghdy, editors. *Parallel Computing: Technology and Practice. PCAT-94. Proceedings of the 7th Australian Transputer and Occam User Group Conference: Wollongong, NSW, Australia, 8–9 November 1994*, volume 43 of *Transputer and occam engineering series*. IOS Press, Postal Drawer 10558, Burke, VA 2209-0558, USA, 1995. ISBN 90-5199-196-7. LCCN ????

Guerrero:1995:CHB

[GN95c] F. Guerrero and J. M. Noras. Customised hardware based on the REDOC III algorithm for high-performance date ciphering. *Lecture Notes in Computer Science*, 975:104–110, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldwasser:1993:ISN

[GO93] S. Goldwasser and R. Ostrovsky. Invariant signatures and non-interactive zero-knowledge proofs are equivalent. *Lecture Notes in Computer Science*, 740:228–245, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Golic:1995:EPC

[GO95] J. D. Golic and L. O'Connor. Embedding and probabilistic correlation attacks on clock-controlled shift registers. *Lecture Notes in Computer Science*, 950:230–243, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldreich:1996:SPS

[GO96a] Oded Goldreich and Rafail Ostrovsky. Software protection and simulation on oblivious RAMs. *Journal of the Association for Computing Machinery*, 43(3):431–473, May 1996. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL http:

//www.acm.org/pubs/toc/Abstracts/jacm/233553.html.

Golic:1996:CCC

[GO96b] J. D. Golic and L. O'Connor. A cryptanalysis of clock-controlled shift registers with multiple steps. *Lecture Notes in Computer Science*, 1029:174–185, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Grosky:1996:NAH

[GO96c] William L. Grosky and Michael Olan. In the news: Apple hopes to ride Internet, multimedia wave back to health; Forum promotes product standards; Asian perspectives on the Internet; focus: The Internet in Malaysia; digital watermarking stakes a claim on the Web; Chinese PC keyboard: a problem with a multimedia solution? Intel gets graphic with new chips. *IEEE MultiMedia*, 3 (2):6–9, Summer 1996. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://dlib.computer.org/mu/books/mu1996/pdf/u2006.pdf.

Goguen:1999:IAS

[Gog99] J. Goguen. An introduction to algebraic semiotics, with application to user interface design. *Lecture Notes in Computer Science*, 1562: 242–291, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Golomb:1967:SRS

[Gol67] S. Golomb. *Shift Register Sequences*. Holden-Day, San Francisco, CA, USA, 1967. xiv + 224 pp. LCCN QA267.5.S4 G6. Portions co-authored with Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales.

Golomb:1982:SRS

[Gol82] S. Golomb. *Shift Register Sequences*. Aegean Park Press, Laguna Hills, CA, USA, revised edition, 1982. ISBN 0-89412-048-4. xvi + 247 pp. LCCN QA267.5.S4 G6 1982. Portions co-authored with Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales.

Goldwasser:1984:PET

[Gol84] Shafrira Goldwasser. *Probabilistic encryption: theory and applications*. Thesis (Ph. D. in Computer Science), Department of Computer Science, University of California, Berkeley, Berkeley, CA, USA, December 1984. iv + 63 pp.

Goldberg:1990:MUA

[Gol90a] David Goldberg. The MITRE user authentication system. In USENIX Association [USE90], pages 1–4. LCCN QA 76.9 A25 U55 1990.

Goldwasser:1990:ACC

[Gol90b] S. Goldwasser, editor. *Advances in cryptology — CRYPTO '88: proceedings*, volume 403 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. CODEN LNCSD9. ISBN 0-387-97196-3 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1988. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0403.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=403`.

Goldwasser:1990:SPS

[Gol90c] Shafi Goldwasser. The search for provably secure cryptosystems. In Pomerance and Goldwasser [PG90], pages 89–113. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

Gollmann:1992:ATC

[Gol92] D. Gollmann. Automata theory and cryptanalysis. In *Cryptography and coding, II (Cirencester, 1989)*, volume 33 of *Inst. Math. Appl. Conf. Ser. New Ser.*, pages 67–74. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1992.

Gollmann:1994:CCC

[Gol94] D. Gollmann. Cryptanalysis of clock controlled shift registers. *Lecture Notes in Computer Science*, 809: 121–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldreich:1995:FCF

[Gol95a] O. Goldreich. Foundation of cryptography — fragments of a book. ????, February 1995. URL `http://theory.lcs.mit.edu/~oded/frag.html`.

Golic:1995:LCS

[Gol95b] J. D. Golic. Linear cryptanalysis of stream ciphers. *Lecture Notes in Computer Science*, 1008:154–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Golic:1996:FLO

[Gol96a] J. D. Golic. Fast low order approximation of cryptographic functions. *Lecture*

Notes in Computer Science, 1070:268–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Golic:1996:CEP

[Gol96b] Jovan Dj. Golić. Constrained embedding probability for two binary strings. *SIAM Journal on Discrete Mathematics*, 9(3):360–364, August 1996. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Gollmann:1996:CA

[Gol96c] D. Gollmann. Cryptographic APIs. *Lecture Notes in Computer Science*, 1029: 290–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gollmann:1996:FSE

[Gol96d] Dieter Gollmann, editor. *Fast software encryption: third International Workshop Cambridge, UK, February 21–23, 1996: proceedings*, volume 1039 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-60865-6 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F38 1996. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1039.htm; http://www.springerlink.com/content/978-3-540-60865-3; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1039.

Goldreich:1997:FMCa

[Gol97a] Oded Goldreich. On the foundations of modern cryptography. *Lecture Notes in Computer Science*, 1294:46–74, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940046.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940046.pdf.

Goldreich:1997:FMCb

[Gol97b] Oded Goldreich. On the foundations of modern cryptography. *CryptoBytes*, 3(2):1, 3–5, Autumn 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n2.pdf.

Goldwasser:1997:NDC

[Gol97c] S. Goldwasser. New directions in cryptography: twenty some years later (or cryptography and complexity theory: a match made in heaven). In

IEEE [IEE97f], pages 314–324. CODEN ASFPDV. ISBN 0-8186-8197-7 (paperback), 0-8186-8198-5 (casebound), 0-8186-8199-3 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 .S92 1997. IEEE catalog number 97CB36150. IEEE Computer Society Press order number PR08197.

Golic:1997:CAA

[Gol97d] J. D. Golic. Cryptanalysis of alleged A5 stream cipher. *Lecture Notes in Computer Science*, 1233:239–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldwasser:1998:C

[Gol98a] S. Goldwasser. Crypto '88. *Lecture Notes in Computer Science*, 1440:87–92, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Golic:1998:RAS

[Gol98b] Jovan Đ. Golić. Recent advances in stream cipher cryptanalysis. *Publ. Inst. Math. (Beograd) (N.S.)*, 64(78):183–204, 1998. ISSN 0350-1302. 50th anniversary of the Mathematical Institute, Serbian Academy of Sciences and Arts (Belgrade, 1996).

Goldreich:1999:MCP

[Gol99a] Oded Goldreich. *Modern cryptography, probabilistic proofs, and pseudorandomness*, volume 17 of *Algorithms and combinatorics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-64766-X. ISSN 0937-5511. xv + 182 pp. LCCN QA76.9.A25 G64 1999.

Golic:1999:SCE

[Gol99b] J. Dj. Golić. Stream cipher encryption of random access files. *Information Processing Letters*, 69(3):145–148, February 12, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Golomb:1999:CNS

[Gol99c] Solomon W. Golomb. On the cryptanalysis of nonlinear sequences [invited paper]. *Lecture Notes in Computer Science*, 1746: 236–242, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gong:1989:SCB

[Gon89] Li Gong. On security in capability-based systems. *Operating Systems Review*, 23(2):56–60, April 1989. CODEN OSRED8. ISSN 0163-5980.

Gong:1992:SRD

[Gon92] Li Gong. A security risk of depending on synchronized clocks. *Operating Systems Review*, 26(1):49–53, January 1992. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Gong:1995:CKH

[Gon95] Li Gong. Collisionful keyed hash functions with selectable collisions. *Information Processing Letters*, 55(3):167–170, August 11, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Gong:1998:JSM

[Gon98] Li Gong. *The Java Security Model: Cryptography, Architectures, APIs, and Implementations*. Addison-Wesley, Reading, MA, USA, 1998. ISBN 0-201-31000-7 (softcover). xiv + 262 pp. LCCN QA76.73.J38 G65 1999. US$36.53. URL `http://www2.awl.com/cseng/javaseries/security.html`.

Good:1979:EWC

[Goo79] I. J. Good. Early work on computers at Bletchley. *Annals of the History of Computing*, 1(1):38–48, July/September 1979. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1979/pdf/a1038.pdf`; `http://www.computer.org/annals/an1979/a1038abs.htm`.

Goodman:1996:LPS

[Goo96] James R. (James Ross) Goodman. Low power scalable encryption for wireless systems. Thesis (M.S.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1996. 114 pp.

Gordon:1985:SPE

[Gor85] John A. Gordon. Strong primes are easy to find. In Beth et al. [BCI85], pages 216–223. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0209.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=209`. Held at the University of Paris, Sorbonne.

Gordon:1993:DDT

[Gor93a] Daniel M. Gordon. Designing and detecting trapdoors for discrete log cryptosystems. *Lecture Notes in Computer Science*, 740: 66–75, 1993. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Gordon:1993:DLU

[Gor93b] Daniel M. Gordon. Discrete logarithms in GF(p) using the number field sieve. *SIAM Journal on Discrete Mathematics*, 6(1):124–138, February 1993. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Goth:1999:NBG

[Got99] Greg Goth. News briefs: Groups duel over new I/O standards; Oracle, Sun team up to dump the OS; bringing the net to mobile appliances; Irish girl invents new E-mail encryption; group releases draft biometric-API specs; Toshiba announces smallest memory chip. *Computer*, 32 (3):18–20, March 1999. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co1999/pdf/r3018.pdf`.

Guajardo:1997:EAE

[GP97] Jorge Guajardo and Christof Paar. Efficient algorithms for elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 1294: 342–356, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ghodosi:1999:RCN

[GP99] H. Ghodosi and J. Pieprzyk. Repudiation of cheating and non-repudiation of Zhang's proxy signature schemes. *Lecture Notes in Computer Science*, 1587: 129–134, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ghodosi:1996:CHG

[GPCSN96] H. Ghodosi, J. Pieprzyk, C. Charnes, and R. Safavi-Naini. Cryptosystems for hierarchical groups. *Lecture Notes in Computer Science*, 1172:275–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gladychev:1998:CRJa

[GPO98a] Pavel Gladychev, Ahmed Patel, and Donal O'Mahony. Cracking RC5 with Java applets. In ACM [ACM98a], page ?? ISBN ???? LCCN ???? URL `http://www.cs.ucsb.edu/conferences/java98/papers/rc5.pdf; http://www.cs.ucsb.edu/conferences/java98/papers/rc5.ps`.

Gladychev:1998:CRJb

[GPO98b] Pavel Gladychev, Ahmed Patel, and Donal O'Mahony.

Cracking RC5 with Java applets. *Concurrency: practice and experience*, 10(11–13):1165–1171, September 1998. CODEN CPEXEI. ISSN 1040-3108. URL http://www3.interscience.wiley.com/cgi-bin/abstract?ID=10050408; http://www3.interscience.wiley.com/cgi-bin/fulltext?ID=10050408&PLACEBO=IE.pdf. Special Issue: Java for High-performance Network Computing.

Goldreich:1998:SCP

[GPR98] O. Goldreich, B. Pfitzmann, and R. L. Rivest. Self-delegation with controlled propagation — or — what if you lose your laptop. *Lecture Notes in Computer Science*, 1462:153–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ghodosi:1997:RMA

[GPSN97] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini. Remarks on the multiple assignment secret sharing scheme. *Lecture Notes in Computer Science*, 1334:72–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ghodosi:1998:SSM

[GPSN98] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini. Secret sharing in multilevel and compartmented groups. *Lecture Notes in Computer Science*, 1438:367–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ghodosi:1998:CCS

[GPSNW98] H. Ghodosi, J. Pieprzyk, R. Safavi-Naini, and H. Wang. On construction of cumulative secret sharing schemes. *Lecture Notes in Computer Science*, 1438:379–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gore:1998:SDC

[GPSV98] Rajeev Goré, Joachim Posegga, Andrew Slater, and Harald Vogt. System description: *card* T^AP: The first theorem prover on a smart card. *Lecture Notes in Computer Science*, 1421:47–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1421/14210047.htm; http://link.springer-ny.com/link/service/series/0558/papers/1421/14210047.pdf.

Gabidulin:1991:INC

[GPT91a] E. M. Gabidulin, A. V. Paramonov, and O. V.

Tretjakov. Ideals over a non-commutative ring and their application in cryptology. *Lecture Notes in Computer Science*, 547: 482–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470482.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0547/05470482.pdf`.

Gabidulin:1991:INR

[GPT91b] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. *Lecture Notes in Computer Science*, 547:482–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gleason:1985:ECP

[GPW85] Andrew M. Gleason, Walter F. Penney, and Ronald E. Wyllys. *Elementary course in probability for the cryptanalyst*, volume 41 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, revised edition, 1985. ISBN 0-89412-072-7. ???? pp. LCCN Z104 .G53 1985.

Guillou:1995:ACE

[GQ95] Louis C. Guillou and J.-J. Quisquater, editors. *Advances in cryptology, EUROCRYPT '95: International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21–25, 1995: proceedings*, volume 921 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-59409-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C794 1995. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0921.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=921`.

Guillou:1998:E

[GQ98] L. C. Guillou and J.-J. Quisquater. Eurocrypt '95. *Lecture Notes in Computer Science*, 1440: 181–190, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Guillou:1991:PTA

[GQW+91] Louis C. Guillou, Jean-Jacques Quisquater, Mike Walker, Peter Landrock, and Caroline Shaer. Precautions taken against various potential attacks in ISO/

IEC DIS 9796 ≪Digital Signature Scheme Giving Message Recovery≫. In Damgård [Dam91a], pages 465–473. CODEN LNCSD9. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1990. DM69.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730465.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730465.pdf.

Gennaro:1997:HSD

[GR97] R. Gennaro and P. Rohatgi. How to sign digital streams. *Lecture Notes in Computer Science*, 1294:180–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gray:1982:ICT

[Gra82] P. E. Gray. Information control I: Technology transfer at issue: The academic viewpoint: Educators believe efforts to limit transfer of knowledge at the university level are likely to weaken the U.S. lead in innovation. *IEEE Spectrum*, 19(5):64–68, May 1982. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Grantham:19xx:FPP

[Graxx] J. Grantham. A Frobenius probable prime test with high confidence. To appear., 19xx. URL http://www.math.uga.edu/~grantham/pseudo/pseudo2.ps.

Goeker:1999:DUC

[GRB99] M. Goeker and T. Roth-Berghofer. Development and utilization of a case-based help-desk support system in a corporate environment. *Lecture Notes in Computer Science*, 1650: 132–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Grehan:1990:CDE

[Gre90] R. Grehan. Cloak and data: An explanation of secret codes and a puzzle to test your skill. *BYTE Magazine*, 15(6):311–312, 314, 316, 318, 320, 322, 324, June 1990. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Greenfield:1994:DPP

[Gre94] Jonathan S. Greenfield. *Distributed programming paradigms with cryptography applications*, volume 870 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc.,

1994. CODEN LNCSD9. ISBN 0-387-58496-X. ISSN 0302-9743 (print), 1611-3349 (electronic). xi + 182 pp. LCCN QA76.9.D5 G74 1994. Revision of the author's doctoral thesis, Syracuse University.

Grossman:1974:GTR

[Gro74] E. Grossman. Group theoretic remarks on cryptographic systems based on two types of addition. Research Report RC-4742, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, February 26, 1974.

Grover:1982:CP

[Gro82] Derrick Grover. Cryptography: a primer. *The Computer Journal*, 25(3):400c–400, August 1982. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/25/3/400-c.full.pdf+html`.

Grosek:1994:RCR

[Gro94] Otokar Grošek. Remarks concerning RSA-cryptosystem exponents. *Mathematica Slovaca*, 44 (2):279–285, 1994. CODEN MASLDM. ISSN 0139-9918 (print), 1337-2211 (electronic). Supplementary issue dedicated to Prof. Š. Schwarz.

Grover:1998:FCP

[Gro98] D. Grover. Forensic copyright protection. *The Computer Law and Security Report*, 14(2):121–122, March/April 1998. CODEN CLSRE8. ISSN 0267-3649. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072121.html`.

Goldschlag:1996:HRI

[GRS96] D. M. Goldschlag, M. G. Reed, and P. F. Syverson. Hiding routing information. In Anderson [And96c], pages 137–150. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054421.html`.

Grundler:1984:DEH

[Gru84] Edward James Grundler. A data encryption hardware software package. Project (M.S.), California State University, Sacramento, Sacramento, CA, USA, 1984. vii + 81 pp.

Grusho:1998:SCI

[Gru98] A. A. Grusho. Subliminal channels and information security in computer systems. *Discrete Mathematics and Applications*, 8 (2):127–133, 1998. CODEN

DMAPEW. ISSN 0924-9265.

Gaines:1978:SSP

[GS78] R. Stockton Gaines and Norman Z. Shapiro. Some security principles and their application to computer security. *Operating Systems Review*, 12(3):19–28, July 1978. CODEN OSRED8. ISSN 0163-5980.

Grollmann:1984:CMP

[GS84] J. Grollmann and A. L. Selman. Complexity measures for public-key cryptosystems. In IEEE [IEE84], pages 495–503. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.

Grollmann:1988:CMP

[GS88] Joachim Grollmann and Alan L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17 (2):309–335, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Girault:1994:LCH

[GS94a] Marc Girault and Jacques Stern. On the length of cryptographic hash-values used in identification schemes. In Desmedt [Des94b], pages 202–215. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390202.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390202.pdf.

Gulliver:1994:ITA

[GS94b] T. Aaron Gulliver and Norman P. Secord, editors. *Information theory and applications: third Canadian workshop, Rockland, Ontario, Canada, May 30–June 2, 1993: proceedings*, volume 793 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 3-540-57936-2 (Berlin), 0-387-57936-2 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN Q350 .C36 1993. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0793.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=793.

Gritzalis:1997:CPO

[GS97] Stefanos Gritzalis and Diomidis Spinellis. Cryptographic protocols over open distributed systems: a taxonomy of flaws and related protocol analysis tools. In *16th International Conference on Computer Safety, Reliability and Security: SAFECOMP '97*, pages 123–137. European Workshop on Industrial Computer Systems: TC-7, Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., September 1997. URL `http://kerkis.math.aegean.gr/~dspin/pubs/conf/1997-SafeComp-Formal/html/doc.html`.

Gong:1998:SSG

[GS98] L. Gong and R. Schemers. Signing, sealing, and guarding Java objects. *Lecture Notes in Computer Science*, 1419:206–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gribomont:1999:SDU

[GS99a] E. Pascal Gribomont and N. Salloum. System description: Using OBDD's for the validation of Skolem verification conditions. *Lecture Notes in Computer Science*, 1632:222–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gysin:1999:GCA

[GS99b] Marc Gysin and Jennifer Seberry. Generalised cycling attacks on RSA and strong RSA primes. *Lecture Notes in Computer Science*, 1587:149–163, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1587/15870149.htm; http://link.springer-ny.com/link/service/series/0558/papers/1587/15870149.pdf`.

Giddy:1994:ACT

[GSN94] J. P. Giddy and R. Safavi-Naini. Automated cryptanalysis of transposition ciphers. *The Computer Journal*, 37(5):429–436, ???? 1994. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Gobioff:1996:SCH

[GSTY96] Howard Gobioff, Sean Smith, J. D. Tygar, and Bennet Yee. Smart Cards in hostile environments. In USENIX [USE96d], pages 23–28. ISBN 1-880446-83-9. LCCN HF5004 .U74 1996. URL `http://www.usenix.org/publications/library/`

proceedings/ec96/gobioff.html.

Goldreich:1999:CSZ

[GSV99] O. Goldreich, A. Sahai, and S. Vadhan. Can statistical zero knowledge be made noninteractive? or on the relationship of SZK and NISZK. In Wiener [Wie99], pages 467–484. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Gafni:1999:EMI

[GSY99] Eli Gafni, Jessica Staddon, and Yiqun Lisa Yin. Efficient methods for integrating traceability and broadcast encryption. In Wiener [Wie99], pages 372–387. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660372.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660372.pdf.

Gramata:1994:MMD

[GTG94] P. Gramata, P. Trebaticky, and E. Gramatova. The MD5 message-digest algorithm in the XILINX FPGA. *Lecture Notes in Computer Science*, 849: 126–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Grehan:1994:BCRa

[GTGW94] Rick Grehan, Tom Thompson, Raymond Ga Cote, and Scott Wallace. Books and CD-ROMs: Levels of secrecy: a look at cryptography, Marvin Minsky on CD-ROM, “plugs,” and visualization of scientific data. *BYTE Magazine*, 19(6):41–??, June 1994. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Gotoh:1990:MRR

[GTS90] Yasuko Gotoh, Kazuo Takaragi, and Ryoichi Sasaki. A method for rapid RSA key generation. *Systems and computers in Japan*, 21(8):11–20, 1990. CODEN SCJAEP. ISSN 0882-1666 (print), 1520-684X (electronic).

Guarini:1904:MTT

[Gua04] Emile Guarini. The Malcotti telecryptograph for telegraphing upon telephone lines. *Scientific American*, 91(12):193–194, September 17, 1904. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v91/n12/pdf/scientificamerican09171904-193a.pdf.

Guan:1987:CAP

[Gua87] Puhua Guan. Cellular automaton public-key cryptosystem. *Complex Systems*, 1(1):51–56, 1987. ISSN 0891-2513.

Guarin:1990:SIA

[Gua90] Maria Victoria Guarin. A study of information authentication and a proposed digital signature scheme. Thesis (M.S. in Engin.), University of Texas at Austin, Austin, TX, USA, 1990. viii + 135 pp.

Guarino:1999:RIC

[Gua99] N. Guarino. The role of identity conditions in ontology design. *Lecture Notes in Computer Science*, 1661: 221–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gudes:1980:DCB

[Gud80] E. Gudes. The design of a cryptography based secure file system. *IEEE Transactions on Software Engineering*, SE-6 (5):411–420, September/ October 1980. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702757`.

Guenther:1998:E

[Gue98a] C. G. Guenther. Eurocrypt '88. *Lecture Notes in Computer Science*, 1440:81–86, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Guergens:1998:SLF

[Gue98b] S. Guergens. SG logic — a formal analysis technique for authentication protocols. *Lecture Notes in Computer Science*, 1361:159–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Guillen:1976:AC

[Gui76] M. Guillen. Automated cryptography. *Science News (Washington, DC)*, 110(12): 188–190, September 18, 1976. CODEN SCNEBK. ISSN 0036-8423 (print), 1943-0930 (electronic).

Guillou:1997:SCR

[Gui97] L. C. Guillou. Some critical remarks on "dynamic data authentication" as specified in EMV '96. *Lecture Notes in Computer Science*, 1318:123–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gullichsen:1983:BHS

[Gul83] Eric Alexander Gullichsen. Bidirectional heuristic search and spectral S-box simplification for the cryptanalysis of the NBS Data Encryption Standard. Thesis (M.Sc.), University of British Columbia, Ottawa, ON, Canada, 1983. 3 microfiches (265 fr.).

Gunther:1988:ASG

[Gun88a] C. Gunther. Alternating step generators controlled by de Bruijn sequences. In Chaum and Price [CP88], pages 5–14. CODEN LNCSD9. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E9631 1987; QA267.A1 L43 no.304. Sponsored by the International Association for Crytologic Research.

Gunther:1988:ACE

[Gun88b] Christoph G. Gunther, editor. *Advances in cryptology — EUROCRYPT '88: Workshop on the Theory and Application of Cryptographic Techniques, Davos, Switzerland, May 25–27, 1988: proceedings*, volume 330 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-50251-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.330; QA76.9.A25 E9641 1988. Sponsored by the International Association for Cryptologic Research.

Gurnsey:1997:CT

[Gur97] John Gurnsey. *Copyright Theft*. Gower, Aldershot; Brookfield, VT, 1997. ISBN 0-566-07631-4. xi + 196 pp. LCCN K1485 .G87 1995; K89 .G87. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1043.html.

Gustafson:1996:SAS

[Gus96] Helen May Gustafson. *Statistical Analysis of Symmetric Ciphers*. Ph.D. thesis, School of Mathematical Sciences, Queensland University of Technology, Brisbane, QLD, Australia, 1996. ???? pp. URL http://www.maths.qut.edu.au/~gustafso/.

Gutmann:1996:SDD

[Gut96] Peter Gutmann. Secure deletion of data from magnetic and solid-state memory. In USENIX [USE96e], page ?? ISBN 1-880446-79-0. LCCN QA76.9.A25 U83 1996. URL http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

Guthery:1998:SC

[Gut98a] Scott Guthery. Smart cards. *;login: the USENIX Association newsletter*, 23(3): ??, May 1998. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/1998-5/guthery.html. Special issue on security.

Gutmann:1998:SGP

[Gut98b] Peter Gutmann. Software generation of practically strong random numbers. In USENIX [USE98d], page ?? ISBN 1-880446-92-8. LCCN QA76.9.A25 U83 1998. URL http://www.cs.auckland.ac.nz/~pgut001/; http://www.cs.auckland.ac.nz/~pgut001/pubs/usenix98.pdf; http://www.usenix.org/publications/library/proceedings/sec98/gutmann.html.

Gutmann:1999:DCS

[Gut99] Peter Gutmann. The design of a cryptographic security architecture. In USENIX [USE99a], page ?? ISBN 1-880446-28-6. LCCN QA76.9.A25 U83 1999. URL http://db.usenix.org/publications/library/proceedings/sec99/gutmann.html.

Guy:1976:HFN

[Guy76] R. K. Guy. How to factor a number. In Hartnell and Williams [HW76], pages 49–89.

Gao:1998:GPO

[GvP98] Shuhong Gao, Joachim von zur Gathen, and Daniel Panario. Gauss periods: orders and cryptographical applications. *Mathematics of Computation*, 67(221): 343–352, 1998. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Griffiths:1976:AMR

[GW76] Patricia P. Griffiths and Bradford W. Wade. An authorization mechanism for a relational database system. *ACM Transactions on Database Systems*, 1(3): 242–255, September 1976. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL http://www.acm.org/pubs/articles/journals/tods/1976-1-3/p242-griffiths/p242-griffiths.pdf; http://www.acm.org/pubs/citations/journals/tods/1976-1-3/p242-griffiths/.

Goldberg:1996:RNB

[GW96] Ian Goldberg and David Wagner. Randomness and the Netscape browser. *Dr. Dobb's Journal of Software Tools*, 21(1):66, 68–70, January 1996. CODEN DDJOEB. ISSN 1044-789X.

Gao:1999:RDF

[GX99] J. Gao and Q. Xu. Rigorous design of a fault diagnosis and isolation algorithm. *Lecture Notes in Computer Science*, 1567: 100–121, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gamow:1958:CAP

[GY58] George Gamow and Martynas Yças. The cryptographic approach to the problem of protein synthesis. In *Das Universum. Unser Bild vom Weltall. (German) [The Universe. Our picture of the Universe]*, page ???? ????, Wiesbaden, Germany, 1958.

Galil:1987:PEA

[GY87] Zvi Galil and Moti Yung. Partitioned encryption and achieving simultaneity by partitioning. *Information Processing Letters*, 26(2): 81–88, October 19, 1987. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Gylden:1931:CEI

[Gyl31] Yves Gyldén. Chifferbyråernas insatser i världskriget till lands. (Swedish) [Cipher bureaus' operations in the World War on land]. Stockholm, Sweden, 1931.

Gylden:1933:CCB

[Gyl34] Yves Gyldén. The contribution of the cryptographic bureaus in the World War. *The Signal Corps Bulletin*, (75–81): ??, November–December 1933–1934. URL `https://archive.org/download/cryptolog_96/cryptolog_96.pdf`.

Gylden:1936:AMC

[Gyl36] Yves Gylden. *Analysis of model C-36 cryptograph from the viewpoint of cryptanalysis*. A. B. Teknik co., Stockholm, Sweden, 1936. 22 pp.

Gylden:1938:APV

[Gyl38] Yves Gylden. *Analysis from the point of view of cryptanalysis of "cryptograph type C-36," provided with six key wheels, 27 slide bars, the latter having movable projections, single or multiple*. A. B. Teknik co., Stockholm, Sweden, 1938. 10 pp.

Gysin:1996:OKC

[Gys96] M. Gysin. A one-key cryptosystem based on a finite nonlinear automaton. *Lecture Notes in Computer Science*, 1029:165–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Garzon:1991:CGG

[GZ91] M. Garzon and Y. Zalcstein. The complexity of Grigorchuk groups with application to cryptography. *Theoretical Computer Science*, 88(1):83–98, September 30, 1991. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Haller:1994:RIA

[HA94a] N. Haller and R. Atkinson. RFC 1704: On Internet authentication, October 1994. URL `ftp://ftp.internic.net/rfc/rfc1704.txt; https://www.math.utah.edu/pub/rfc/rfc1704.txt`. Status: INFORMATIONAL.

Hendessi:1994:SAA

[HA94b] F. Hendessi and M. R. Aref. A successful attack against the DES. *Lecture Notes in Computer Science*, 793:78–90, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hollaar:1996:LRD

[HA96] L. Hollaar and A. Asay. Legal recognition of digital-signatures. *IEEE Micro*, 16 (3):44–45, May/June 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (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.

Haddon:1984:BRS

[Had84] Bruce K. Haddon. Book review of "Security, IFIP/Sec'83: proceedings of the first security conference" North-Holland Publishing Co. 1983. *Operating Systems Review*, 18(3): 14, July 1984. CODEN OSRED8. ISSN 0163-5980. See [Fêa83].

Hagelin:1998:SHC

[Hag98] Boris C. W. Hagelin. The story of the Hagelin cryptos. In Deavours et al. [DKK+98], pages 477–515. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Hoffman:1994:CP

[HAHH94] Lance J. Hoffman, Faraz A. Ali, Steven L. Heckler, and Ann Huybrechts. Cryptography policy. *Communications of the Association for Computing Machinery*, 37(9):109–117, September 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/184079.html.

Hammer:1971:SSC

[Ham71] Carl Hammer. Signature simulation and certain cryptographic codes. *Communications of the Association* *for Computing Machinery*, 14(1):3–14, January 1971. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Hamming:1980:CIT

[Ham80] R. W. (Richard Wesley) Hamming. *Coding and information theory*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1980. ISBN 0-13-139139-9. xii + 239 pp. LCCN QA268 .H35 1980. US$19.95.

Hamming:1986:CIT

[Ham86] R. W. (Richard Wesley) Hamming. *Coding and information theory*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, second edition, 1986. ISBN 0-13-139072-4. xii + 259 pp. LCCN QA268 .H35 1986. US$36.95.

Hamilton:19xx:PC

[Hamxx] V. Hamilton. Personal communication. ????, 19xx.

Hansen:1994:MLD

[Han94] Per Brinch Hansen. Multiple-length division revisited: a tour of the minefield. *Software—Practice and Experience*, 24(6):579–601, June 1994. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic). This paper derives an algorithm for division of long integers, and implements it as a literate program, although without identifier cross-references.

Hancock:1995:ECI

[Han95] Bill Hancock. Export of cryptographic information from the US: a brief look at the problems. *Network Security*, 1995(10):9–11, October 1995. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/1353485896897583`.

Hancock:1997:UCE

[Han97] Bill Hancock. The US cryptographic export debate — round five? *Network Security*, 1997(3):6–7, March 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485897830413`.

Hancock:1999:ECI

[Han99] Bill Hancock. Export of cryptographic information from the USA: A brief look at the problems. *Network Security*, 1999(5):17–19, May 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485800800203`.

Hardjono:1990:RED

[Har90] Thomas Hardjono. Record encryption in distributed databases. In *Advances in cryptology—AUSCRYPT '90 (Sydney, 1990)*, volume 453 of *Lecture Notes in Comput. Sci.*, pages 386–395. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990.

Harari:1991:CCS

[Har91] S. Harari. A correlation cryptographic scheme. *Lecture Notes in Computer Science*, 514:180–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hart:1994:DSC

[Har94] George W. Hart. To decode short cryptograms. *Communications of the Association for Computing Machinery*, 37(9):102–108, September 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/184078.html`.

Harpes:1996:CIB

[Har96a] Carlo Harpes. *Cryptanalysis of iterated block ciphers*. Thesis (Ph.D.), Eidgenossische Technische Hochschule, Zurich, Switzerland, 1996. xi + 171 pp. Published y Hartung-Gorre, Konstanz, Switzerland.

Harris:1996:E

[Har96b] Robert Harris. *Enigma*. Ivy Books, New York, NY, USA, 1996. ISBN 0-8041-1548-6.

Haskett:1984:PAU

[Has84] James A. Haskett. Pass-algorithms: a user validation scheme based on knowledge of secret algorithms. *Communications of the Association for Computing Machinery*, 27(8): 777–781, 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Haastad:1987:OWP

[Hås87] Johan Håstad. One-way permutations in NC^0. *Information Processing Letters*, 26(3):153–155, November 23, 1987. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Haastad:1988:SSM

[Hås88] Johan Håstad. Solving simultaneous modular equations of low degree. *SIAM Journal on Computing*, 17 (2):336–341, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Haselberger:1995:DRB

[Has95] Lothar Haselberger. Deciphering a Roman blueprint. *Scientific American*, 272 (6):84–?? (Intl. ed. 56–??), June 1995. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Hasan:1999:LTB

[Has99] M. A. Hasan. Look-up table based large finite field multiplication in memory constrained cryptosystems (extended abstract). *Lecture Notes in Computer Science*, 1746:213–221, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hatefi:1996:MRE

[Hat96] Farid Hatefi. Media reviews: Encryption technology explained: *Building in Big Brothers — The Cryptography Policy Debate*, Lance J. Hoffman, Editor (Springer-Verlag, 1995, $29.95, ISBN 0-387-94441-9); on the shelf. *IEEE MultiMedia*, 3(4):87–88, Winter 1996. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL `http://dlib.computer.org/mu/books/mu1996/pdf/u4087.pdf`.

Hatefi:1997:AED

[Hat97] Farid G. Hatefi. Application of encryption/decryption in network management. Thesis (M.S.), Arizona State University, Tempe, AZ, USA, 1997. xi + 112 pp.

Haugen:1974:RSS

[Hau74] Einar Haugen. The rune stones of Spirit Pond, Maine. *Visible Language*, VIII(1):33–64, Winter 1974. CODEN VSLGAO. ISSN 0022-2224 (print), 2691-5529 (electronic). URL `https://s3-us-west-2.amazonaws.com/visiblelanguage/pdf/V8N1_1974_E.pdf`.

Hawkes:1998:DWK

[Haw98a] P. Hawkes. Differential-linear weak key classes of IDEA. *Lecture Notes in Computer Science*, 1403: 112–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hawkes:1998:DLW

[Haw98b] Philip Hawkes. Differential-linear weak key classes of IDEA. *Lecture Notes in Computer Science*, 1403: 112–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030112.htm; http://link.springer-ny.com/link/service/series/`

0558/papers/1403/14030112.pdf.

Hutter:1999:DCI

[HB99] D. Hutter and A. Bundy. The design of the CADE-16 inductive theorem prover contest. *Lecture Notes in Computer Science*, 1632: 374–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hughes:1999:PFS

[HBKL99] R. J. Hughes, W. T. Buttler, P. G. Kwiat, and S. K. Lamoreaux. Practical free-space quantum cryptography. *Lecture Notes in Computer Science*, 1509: 200–213, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Huang:1988:SWP

[HC88] Yue Jiang Huang and Fred Cohen. Some weak points of one fast cryptographic checksum algorithm and its improvement. *Computers and Security*, 7(5):503–505, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888902040.

Hu:1995:YCE

[HC95a] Ping Hu and Bruce Christianson. Is your computing environment secure?: security problems with interrupt handling mechanisms. *Operating Systems Review*, 29(4):87–96, October 1995. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Hwang:1995:SSA

[HC95b] Tzonelih Hwang and Yung-Hsiang Chen. On the security of SPLICE/AS — the authentication system in WIDE Internet. *Information Processing Letters*, 53(2):97–101, January 27, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:1996:DSS

[HC96] S.-J. Hwang and C.-C Chang. A dynamic secret sharing scheme with cheater detection. *Lecture Notes in Computer Science*, 1172:48–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hwang:1998:EMS

[HCC98] Shin-Jia Hwang, Chien-Yuang Chen, and Chin-Chen Chang. An encryption/multisignature scheme with specified receiving groups. *International Journal of Computer Systems Science and Engineering*, 13 (2):109–112, March 1998.

CODEN CSSEEI. ISSN 0267-6192.

Hernandez:1999:DAV

[HCDC99] M. Hernandez, J. Cabrera, A. Dominguez, and M. Castrillon. DESEO: An active vision system for detection, tracking and recognition. *Lecture Notes in Computer Science*, 1542: 376–391, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hwang:1996:SAA

[HCY96a] S.-J. Hwang, C.-C. Chang, and W.-P. Yang. Some active attacks on fast server-aided secret computation protocols for modular exponentiation. *Lecture Notes in Computer Science*, 1029: 215–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hwang:1996:AES

[HCY96b] Shin-Jia Hwang, Chin-Chen Chang, and Wei-Pang Yang. Authenticated encryption schemes with message linkage. *Information Processing Letters*, 58(4): 189–194, May 27, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

He:1996:HFR

[HD96a] J. He and E. Dawson. How to fairly reconstruct a shared secret. *Lecture Notes in Computer Science*, 1029:115–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

He:1996:NKE

[HD96b] J. He and E. Dawson. A new key escrow cryptosystem. *Lecture Notes in Computer Science*, 1029:105–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

He:1992:IKB

[He92] Jing Min He. An improved knapsack-based public key cryptosystem. *J. Tsinghua Univ.*, 32(4):86–91, 1992. CODEN QDXKE8. ISSN 1000-0054.

Huang:1998:FAI

[HE98] Mao Lin Huang and P. Eades. A fully animated interactive system for clustering and navigating huge graphs. *Lecture Notes in Computer Science*, 1547: 374–383, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hedberg:1997:FIC

[Hed97] Sara Reese Hedberg. Up front: HP's international cryptography framework: compromise or threat? *Computer*, 30(1):28–30, January 1997. CODEN CPTRB4. ISSN 0018-9162

(print), 1558-0814 (electronic).

Hartung:1998:DWM

[HEG98] Frank Hartung, Peter Eisert, and Bernd Girod. Digital watermarking of MPEG-4 facial animation parameters. *Computers and Graphics*, 22(4):425–435, July–August 1, 1998. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.elsevier.com/cas/tree/store/cag/sub/1998/22/4/566.pdf.

Heidel:1676:JTP

[Hei76] Wolfgango Ernesto Heidel. *Johannis Trithemii primo Spanheimensis deinde Divi Jacobi Peapolitani abbatis Steganographia: quae hucusq[ue] a nemine intellecta sed passim ut supposititia, perniciosa, magica & necromantica rejecta, elusa, damnata & sententiam inquisitionis passa, nunc tandem vindicata, reserata et illustrata ubi post vindicias Trithemii clarissime explicantur conjurationes spirituum ex Arabicis, Hebraicis, Chaldaicis & Graecis spirituum nominibus juxta quosdam conglobatae, aut secundum alios ex barbaris & nihil significantibus verbis concinnatae: deinde solvuntur & exhibentur artificia nova steganographica a Trithemio in literis ad Arnoldum Bostium & Polygraphia promissa, in hunc diem a nemine capta, sed pro paradoxis & impossibilibus habita & summe desiderata*. Wormatiense, Moguntiae. Sumptibus Joannis Petri Zubrodt, 1676. 8 + 394 (or 396) + 4 pp. LCCN Z103 .T84 1676. Includes Heidel's life of Trithemius and his vindication of the Steganographia.

Heideman:1996:SIT

[Hei96a] G. H. L. M. Heideman, editor. *17th Symposium on Information Theory in the Benelux, Enschede, The Netherlands, May, 1996*. Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, The Netherlands, 1996. ISBN 90-365-0812-6. LCCN ????

Heintze:1996:SDF

[Hei96b] N. Heintze. Scalable document fingerprinting. In USENIX [USE96d], pages 191–200. ISBN 1-880446-83-9. LCCN HF5004 .U74 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054137.html.

Hellman:1976:SPN

[Hel76] M. E. Hellman. Statement to participants at

NBS workshop on cryptography in support of computer security. Unpublished memorandum, ????, ????, September 21, 1976.

Hellman:1979:WTI

[Hel79a] M. E. Hellman. I. 'DES will be totally insecure within ten years'. *IEEE Spectrum*, 16(7):32–40, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Hellman:1979:MPK

[Hel79b] Martin E. Hellman. The mathematics of public-key cryptography. *Scientific American*, 241(2):146–157 (Intl. ed. 130–139), August 1979. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Hellman:1981:ACA

[Hel81] M. E. Hellman. Another cryptanalytic attack on "A cryptosystem for multiple communication" [Inform. Process. Lett. **10**(4–5), 5 July 1980, pp. 180–183]. *Information Processing Letters*, 12(4):182–183, August 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [LM80, Mei81].

Held:1993:TSD

[Hel93] Gilbert Held. *Top secret data encryption techniques.* Howard W. Sams, Indianapolis, IN 46268, USA, 1993. ISBN 0-672-30293-4. 218 pp. LCCN QA76.9.A25H43 1993.

Helleseth:1994:ACE

[Hel94] Tor Helleseth, editor. *Advances in cryptology, EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 23–27, 1993: proceedings*, volume 765 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 3-540-57600-2 (Berlin), 0-387-57600-2 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1993. DM86.00. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0765.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=765`.

Held:1998:ARU

[Hel98a] Gilbert Held. Authenticating remote users. *Sys Admin: The Journal for UNIX Systems Administrators*, 7 (8):57, 59–62, August 1998. CODEN SYADE7. ISSN 1061-2688. URL `http://www.samag.com/`.

Held:1998:LET

[Hel98b] Gilbert Held. *Learn encryption techniques with BASIC and C++*. Wordware Pub., Plano, TX, USA, 1998. ISBN 1-55622-598-9 (paperback). ?? pp. LCCN QA76.9.A25H42 1998.

Helleseth:1998:E

[Hel98c] T. Helleseth. Eurocrypt '93. *Lecture Notes in Computer Science*, 1440: 153–158, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Henry:1981:BJB

[Hen81] P. S. Henry. B.S.T.J. briefs: Fast decryption algorithm for the knapsack cryptographic system. *The Bell System Technical Journal*, 60(5):767–773, May–June 1981. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol60/bstj60-5-767.pdf`.

Henry:1982:FDA

[Hen82] Paul S. Henry. Fast decryption algorithm for the knapsack cipher. *Computers and Security*, 1(1):80–83, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900293`.

Hong:1998:DAS

[HEQL98] S.-H. Hong, P. Eades, A. Quigley, and S.-H. Lee. Drawing algorithms for series-parallel digraphs in two and three dimensions. *Lecture Notes in Computer Science*, 1547: 198–209, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Herlestam:1978:CRS

[Her78] Tore Herlestam. Critical remarks on some public-key cryptosystems. *BIT*, 18(4):493–496, December 1978. CODEN NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=18&issue=4&spage=493`.

Hershey:1981:DLP

[Her81] J. E. (John E.) Hershey. The discrete logarithm public cryptographic system. NTIA report 81-81, PB82-130097, U.S. Dept. of Commerce, National Telecommunications and Information Administration, Washington, DC, USA (??), September 1981. iv + 40 pp.

Hersch:1989:DSA

[Her89] Jeffrey Stuart Hersch. Digital signature analysis of radar reflections for the assessment of concrete bridge deck deterioration. Thesis (M.S.), Massachusetts Institute of Technology, Department of Civil Engineering, Cambridge, MA, USA, 1989. 165 pp. Supervised by Kenneth R. Maser and Alexander Slocum.

Hess:1997:PKC

[Hes97] E. Hess. Public-key cryptosystems based on elliptic curves — an evolutionary approach. *Lecture Notes in Computer Science*, 1355: 118–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hollan:1997:AMP

[HF97] James D. Hollan and James D. Foley, editors. *ACM Multimedia '97: proceedings: November 9–13, 1997, Seattle, Washington, USA*. ACM Press, New York, NY 10036, USA, 1997. ISBN 0-201-32232-3, 0-89791-991-2 (ACM). LCCN QA76.575.A36 1997. ACM order number 433971.

Hardy:1985:ECC

[HFL+85] John M. Hardy, Dorothy W. Fuller, Douglas R. Long, Jane C. Hartin, and Faye Davis. *Electronic cryptographic communications equipment specialist (AFSC 30650)*. Extension Course Institute, Air University, ????, 1985. various pp.

Housley:1999:RIX

[HFPS99] R. Housley, W. Ford, W. Polk, and D. Solo. RFC 2459: Internet X.509 public key infrastructure certificate and CRL profile, January 1999. URL `ftp://ftp.internic.net/rfc/rfc2459.txt`; `https://www.math.utah.edu/pub/rfc/rfc2459.txt`. Status: PROPOSED STANDARD.

Hartung:1996:DWR

[HG96] Frank H. Hartung and Bernd Girod. Digital watermarking of raw and compressed video. In Ohta [Oht96], pages 205–213. CODEN PSISDG. ISBN 0-8194-2356-4. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TA1637 .D53 1996.

Handschuh:1997:CCS

[HG97a] H. Handschuh and H. Gilbert. chi02 cryptanalysis of the SEAL encryption algorithm. *Lecture Notes in Computer Science*, 1267: 1–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Handschuh:1997:CSE

[HG97b] Helena Handschuh and Henri Gilbert. χ^2 cryptanalysis of the SEAL encryption algorithm. *Lecture Notes in Computer Science*, 1267:1–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670001.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670001.pdf.

Hartung:1997:CPV

[HG97c] F. Hartung and B. Girod. Copyright protection in video delivery networks by watermarking of pre-compressed video. *Lecture Notes in Computer Science*, 1242:423–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hartung:1997:WME

[HG97d] F. Hartung and B. Girod. Watermarking of MPEG-2 encoded video without decoding and re-encoding. In Freeman et al. [FJV97], pages 264–273. ISBN 0-8194-2431-5. LCCN TS510.S63 v.3020. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/063131.html.

Hartung:1997:DWM

[HG97e] Frank Hartung and Bernd Girod. Digital watermarking of MPEG-2 coded video in the bitstream domain. In IEEE [IEE97d], pages 2621–2624. CODEN IPRODJ. ISBN 0-8186-7920-4 (casebound), 0-8186-7919-0, 0-8186-7921-2 (microfiche). ISSN 0736-7791. LCCN TK 7882 S65 I16 1997. Five volumes. IEEE catalog number 97CB36052. IEEE Computer Society Press order number PR07919.

Hartung:1998:WUA

[HG98] F. Hartung and B. Girod. Watermarking of uncompressed and compressed video. *Signal Processing*, 66(3):283–301, May 1998. CODEN SPRODR. ISSN 0165-1684. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073135.html.

Hoornaert:1985:EHI

[HGD85] Frank Hoornaert, Jo Goubert, and Yvo Desmedt. Efficient hardware implementation of the DES. In Blakley and Chaum [BC85], pages 147–173. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=147. CRYPTO 84: a Workshop on the Theory and Application of

Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Haddar:1998:ISI

[HGHD98] N. Haddar, F. Gargouri, A. B. Hamadou, and C. F. Ducateau. Information systems integration: Some principles and ideas. *Lecture Notes in Computer Science*, 1415:79–88, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hall:1998:RAA

[HGS98] C. Hall, I. Goldberg, and B. Schneier. Reaction attacks against several public-key cryptosystems. Counterpane systems report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. URL `http://www.counterpane.com/reaction_attacks.html`.

Hinsley:1979:BISb

[HH79] F. H. (Francis Harry) Hinsley and Michael Eliot Howard. *British intelligence in the Second World War: its influence on strategy and operations*. Cambridge University Press, New York, NY, USA, 1979. ISBN 0-521-22940-5 (vol. 1). various pp. LCCN D810.S7 H47 1979b. Vols. 3-4 in series: History of the Second World War. Vol. 4 has subtitle: Security and counterintelligence; Vol. 5 has subtitle: Strategic deception.

Hofmann:1994:RQC

[HH94] H. F. Hofmann and R. Holbein. Reaching out for quality: Considering security requirements in the design of information systems. *Lecture Notes in Computer Science*, 811:105–118, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hughes:1998:AJC

[HH98] Merlin Hughes and Conrad Hughes. *Applied Java Cryptography*. Manning Publications, Greenwich, CT, USA, May 1998. ISBN 1-884777-63-5. US$37.

Husemann:1999:OTY

[HH99] Dirk Husemann and Reto Hermann. OpenCard: Talking to your smart card. *IEEE Concurrency*, 7(3):53–57, July/September 1999. CODEN IECMFX. ISSN 1092-3063 (print), 1558-0849 (electronic). URL `http://dlib.computer.org/pd/books/pd1999/pdf/p3053.pdf`; `http://www.computer.org/concurrency/pd1999/p3053abs.htm`.

Hutton:1999:ASM

[HHD99] T. J. Hutton, P. Hammond, and J. C. Davenport. Active shape models for customised prosthesis design. *Lecture Notes in Computer Science*, 1620:448–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Harn:1989:PAU

[HHL89] L. Harn, D. Huang, and C. S. Laih. Password authentication using public-key cryptography. *Computers and Mathematics with Applications*, 18(12):1001–1017, ???? 1989. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/089812218990028X.

Han:1993:TCC

[HHT93] Y. Han, L. A. Hemaspaandra, and T. Thierauf. Threshold computation and cryptographic security. *Lecture Notes in Computer Science*, 762:230–239, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Han:1997:TCC

[HHT97] Yenjo Han, Lane A. Hemaspaandra, and Thomas Thierauf. Threshold computation and cryptographic security. *SIAM Journal on Computing*, 26(1):59–78, February 1997. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/toc/SICOMP/26/1.

Hochberger:1999:CDM

[HHW99] C. Hochberger, R. Hoffman, and S. Waldschmidt. CDL++ for the description of moving objects in cellular automata. *Lecture Notes in Computer Science*, 1662:428–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Harn:1993:OTP

[HHY93] Lein Harn and Lin Hung-Yu. An oblivious transfer protocol and its application for the exchange of secrets. *Lecture Notes in Computer Science*, 739:312–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hirose:1997:CKD

[HI97] Shouichi Hirose and Katsuo Ikeda. A conference key distribution system for the star configuration based on the discrete logarithm problem. *Information Processing Letters*, 62(4):189–192, June 11, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Higenbottam:1973:CC

[Hig73] Frank Higenbottam. *Codes and ciphers*. English Universities Press, London, UK, 1973. ISBN 0-340-12493-8. 180 (est.) pp. LCCN ????

Highland:1983:BRCb

[Hig83] Harold Joseph Highland. Book review: *Codes, ciphers and computers: an introduction to information security*: Bruce Bosworth: Rochelle Park NJ: Hayden Book Company, Inc., 1982. viii + 259 pp., $13.95. *Computers and Security*, 2(1): 83–84, January 1983. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488390041X.

Highland:1987:CC

[Hig87a] Harold Joseph Highland. Cipher cracking. *Computers and Security*, 6(3): 205, June 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887901015.

Highland:1987:DES

[Hig87b] Harold Joseph Highland. Data encryption standard II? *Computers and Security*, 6(3):195–196, June 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900952.

Highland:1987:EP

[Hig87c] Harold Joseph Highland. Encryption package. *Computers and Security*, 6(3): 199–202, June 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900988.

Highland:1987:HSY

[Hig87d] Harold Joseph Highland. How secure are your encryption keys? *Computers and Security*, 6(2):99–100, April 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900757.

Highland:1987:HEM

[Hig87e] Harold Joseph Highland. How to evaluate microcomputer encryption software and hardware. *Computers and Security*, 6(3):229–244, June 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887901040.

Highland:1988:PEM

[Hig88a] Esther H. Highland. Picking encryption method is no time for secrets: Harold Joseph Highland, Government Computer News, April 29, 1988, p. 39. *Computers and Security*, 7(4): 431, August 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888906360.

Highland:1988:RRC

[Hig88b] Esther H. Highland. A redundancy reducing cipher: Peter Wayner, Cryptologia, April 1988, pp. 107–112. *Computers and Security*, 7(4):431–432, August 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888906414.

Highland:1988:TSC

[Hig88c] Esther H. Highland. Top secret — concepts and implementation. *Computers and Security*, 7(3): 329, June 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888901034.

Highland:1988:TSV

[Hig88d] Esther H. Highland. Top secret, and vulnerable: John Markoff, The New York Times, April 25, 1988, pp. D1, D4. *Computers and Security*, 7(4):430, August 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888906311.

Highland:1988:EAE

[Hig88e] Harold Joseph Highland. Encryption, attacks and ethics. *Computers and Security*, 7(1):5–6, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888904890.

Highland:1988:SIT

[Hig88f] Harold Joseph Highland. Secretdisk II — transparent automatic encryption. *Computers and Security*, 7 (1):27–34, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888904981.

Highland:1989:SDI

[Hig89] Harold Joseph Highland. Secret disk II — administrator. *Computers* *and Security*, 8(7):563–568, November 1989. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404889900485.

Highland:1997:HCV

[Hig97a] H. J. Highland. A history of computer viruses. *Computers and Security*, 16(5):412–438, ???? 1997. CODEN CPSEDU. ISSN 0167-4048. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064343.html.

Highland:1997:PRC

[Hig97b] H. J. Highland. Procedures to reduce the computer virus threat. *Computers and Security*, 16(5):439–449, ???? 1997. CODEN CPSEDU. ISSN 0167-4048. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064345.html.

Hill:1929:CAA

[Hil29] Lester S. Hill. Cryptography in an algebraic alphabet. *American Mathematical Monthly*, 36(6):306–312, June/July 1929. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Hill:1931:CCL

[Hil31] Lester S. Hill. Concerning certain linear transformation apparatus of cryptography. *American Mathematical Monthly*, 38(3):135–154, March 1931. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Hiltgen:1994:CRC

[Hil94] Alain P. L. Hiltgen. *Cryptographically relevant contributions to combinational complexity theory*. Hartung-Gorre Verlag, Konstanz, Switzerland, 1994. ISBN 3-89191-745-7. xi + 129 pp. LCCN QA76.9.A25 H55 1994.

Hill:1997:MTY

[Hil97] Paul Hill. More than you ever wanted to know about NT login authentication. *;login: the USENIX Association newsletter*, 22(4):18–19, August 1997. CODEN LOGNEM. ISSN 1044-6397.

Haastad:1999:PGO

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, August 1999. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/24470.

Hinsley:1993:BIS

[Hin93] F. H. (Francis Harry) Hinsley. *British intelligence in the Second World War*. Cambridge University Press, New York, NY, USA, abridged edition, 1993. ISBN 0-521-44304-0. xiii + 628 pp. LCCN D810.S7 H49 1993. Abridgement of British intelligence in the Second World War originally published in 5 v. between 1979–1990.

Hirschfeld:1993:MER

[Hir93] R. Hirschfeld. Making electronic refunds safer. *Lecture Notes in Computer Science*, 740:106–112, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hirschfeld:1997:FCF

[Hir97] Rafael Hirschfeld, editor. *Financial cryptography: First International Conference, FC '97, Anguilla, British West Indies, February 24–28, 1997: proceedings*, volume 1318 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-63594-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 1997.

Hirschfeld:1998:FCS

[Hir98] Rafael Hirschfeld, editor. *Financial Cryptography: Second International Conference, FC '98, Anguilla, British West Indies, February 23–25, 19987: proceedings*, volume 1465 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-64951-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN HG1710 .F35 1998.

Hitt:1943:MSM

[Hit43] Parker Hitt. *Manual for the solution of military ciphers ... For use in Donald D. Millikin's cryptography and cryptanalysis classes*. New York University Bookstore, New York, NY, USA, 1943. viii + 101 + 22 pp.

Helman:1999:DPE

[HJ99] D. R. Helman and J. Jaja. Designing practical efficient algorithms for symmetric multiprocessors. *Lecture Notes in Computer Science*, 1619:37–56, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

HJH:1985:BRK

[HJH85] HJH. Book review: *Kahn on codes: Secrets of the new* *cryptology*: David Kahn New York: Macmillan Publishing Company, 1984. 344 + viii pages, $19.95. *Computers and Security*, 4(3): 247, September 1985. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404885900379`.

Herzberg:1997:PPK

[HJJ+97] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. Proactive public key and signature systems. In ???? [???97], page ??

Herzberg:19xx:PPK

[HJJ+xx] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. Proactive public key and signature systems. ????, 19xx. URL `http://theory.lcs.mit.edu/cis/cis-publications.html`.

Herzberg:1995:PSS

[HJKY95] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing, or: How to cope with perpetual leakage. In Coppersmith [Cop95d], pages 339–352. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=963`. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Hillenbrand:1999:SDW

[HJL99] T. Hillenbrand, A. Jaeger, and B. Loechner. System description: Waldmeister — improvements in performance and ease of use. *Lecture Notes in Computer Science*, 1632:232–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hong:1997:IAU

[HJPB97] L. Hong, A. Jain, S. Pankanti, and R. Bolle. Identity authentication using fingerprints. *Lecture Notes in Computer Science*, 1206: 103–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Huehnlein:1998:CBN

[HJPT98a] D. Huehnlein, M. J. Jacobson, S. Paulus, and T. Takagi. A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption. *Lecture Notes in Computer Science*, 1403: 294–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Huhnlein:1998:CBN

[HJPT98b] Detlef Hühnlein, Michael J. Jacobson, Jr., Sachar Paulus, and Tsuyoshi Takagi. A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption. *Lecture Notes in Computer Science*, 1403: 294–307, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030294.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030294.pdf`.

Hauser:1996:RSP

[HJT+96] Ralf Hauser, Philippe Janson, Gene Tsudik, Els Van Herreweghen, and Refik Molva. Robust and secure password and key change method. *Journal of Computer Security*, 4(1):97–111, ???? 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Herlea:1999:SBR

[HJTW99] D. E. Herlea, C. M. Jonker, J. Treur, and N. J. E. Wijngaards. Specification of behavioural requirements within compositional multi-agent system design. *Lecture Notes in Computer Science*, 1647:8–27, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Harn:1990:EPE

[HK90] Lein Harn and Thomas Kiesler. An efficient probabilistic encryption scheme. *Information Processing Letters*, 34(3):123–129, April 9, 1990. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Halevi:1997:MSM

[HK97] Shai Halevi and Hugo Krawczyk. MMH: Software message authentication in the Gbit/second rates. *Lecture Notes in Computer Science*, 1267: 172–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670172.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670172.pdf`.

Hevia:1998:STD

[HK98] Alejandro Hevia and Marcos Kiwi. Strength of two Data Encryption Standard implementations under timing attacks. *Lecture Notes in Computer Science*, 1380:192–205, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1380/13800192.htm; http://link.springer-ny.com/link/service/series/0558/papers/1380/13800192.pdf.

Halevi:1999:PKC

[HK99a] Shai Halevi and Hugo Krawczyk. Public-key cryptography and password protocols. *ACM Transactions on Information and System Security*, 2(3):230–268, August 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org/pubs/citations/journals/tissec/1999-2-3/p230-halevi/.

Halfmann:1999:ESP

[HK99b] Udo Halfmann and Winfried E. Kühnhauser. Embedding security policies into a distributed computing environment. *Operating Systems Review*, 33(2):51–64, April 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Haynes:1999:VDS

[HK99c] John Earl Haynes and Harvey Klehr. *Venona: decoding Soviet espionage in America*. Yale University Press, New Haven, CT, USA, 1999. ISBN 0-300-07771-8. xiii + 487 pp. LCCN JK2391.C5 H39 1999.

Hevia:1999:STD

[HK99d] Alejandro Hevia and Marcos Kiwi. Strength of two Data Encryption Standard implementations under timing attack. *ACM Transactions on Information and System Security*, 2(4):416–437, November 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org/pubs/citations/journals/tissec/1999-2-4/p416-hevia/.

Hromkovic:1994:CDC

[HKL94] J. Hromkovic, J. Karhumaeki, and A. Lepistoe. Comparing descriptional and computational complexity of infinite words. *Lecture Notes in Computer Science*, 812:169–182, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Harpes:1995:GLC

[HKM95] C. Harpes, G. G. Kramer, and J. L. Massey. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. *Lecture Notes in Computer Science*, 921:24–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hachez:1999:IFA

[HKQ99] G. Hachez, François Koeune, and J.-J. Quisquater. Implementation of four AES candidates on two smart cards. In National Institute of Standards and Technology [Nat99b], page 22. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf2/Koeune.pdf`. Only the slides for the conference talk are available.

Hall:1999:CS

[HKRS99] C. Hall, J. Kelsey, V. Rijmen, and B. Schneier. Cryptanalysis of SPEED. *Lecture Notes in Computer Science*, 1556:319–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Haber:1995:HDD

[HKS95] Stuart Haber, Burt Kaliski, and Scott Stornetta. How do digital time-stamps support digital signatures. *CryptoBytes*, 1(3):14–15, Autumn 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf`.

Hofmeister:1997:CKS

[HKS97a] T. Hofmeister, M. Krause, and H. U. Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Lecture Notes in Computer Science*, 1276:176–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hofmeister:1997:COS

[HKS97b] T. Hofmeister, M. Krause, and H. U. Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Lecture Notes in Computer Science*, 1276:176–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hall:1998:CS

[HKSW98] C. Hall, J. Kelsey, B. Schneier, and D. Wagner. Cryptanalysis of SPEED. *Lecture Notes in Computer Science*, 1465:309–310, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/speed-sac.html`. Fifth Annual Workshop on Selected Areas in Cryptography, Springer-Verlag, August 1998, to appear.

He:1988:SDK

[HL88] Jing Min He and Kai Cheng Lu. The security and design of knapsack public key cryptosystems. *J. Tsinghua Univ.*, 28(1):89–97, 1988. CODEN QDXKE8. ISSN 1000-0054.

Hauser:1992:VMA

[HL92] Ralf C. Hauser and E. Stewart Lee. Verification and modelling of authentication protocols. *Lecture Notes in Computer Science*, 648: 141–??, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Harn:1993:SGS

[HL93a] L. Harn and H.-Y. Lin. An l-span generalized secret sharing scheme. *Lecture Notes in Computer Science*, 740:558–565, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Herzberg:1993:PRC

[HL93b] A. Herzberg and M. Luby. Public randomness in cryptography. *Lecture Notes in Computer Science*, 740: 421–432, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Han:1999:VFG

[HL99] Y. Han and K. Lee. Virtual function generators: Representing and reusing underlying design concepts in conceptual synthesis of mechanisms for function generation. *Lecture Notes in Computer Science*, 1650: 453–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hwang:1999:CDC

[HLC99] Ren-Junn Hwang, Wei-Bin Lee, and Chin-Chen Chang. A concept of designing cheater identification methods for secret sharing. *The Journal of Systems and Software*, 46(1):7–11, April 1, 1999. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.elsevier.com/cas/tree/store/jss/sub/1999/46/1/6111.pdf`.

Hwang:1995:TAN

[HLL+95] Tzonelih Hwang, Narn-Yih Lee, Chuan-Ming Li, Ming-Yung Ko, and Yung-Hsiang Chen. Two attacks on Neuman-Stubblebine authentication protocols. *Information Processing Letters*, 53(2):103–107, January 27, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:1996:SCW

[HLLC96] Tzonelih Hwang, Narn-Yih Lee, Chuan-Ming Li, and Chin-Chen Chang. On the security of Chang and Wu's broadcasting cryptosystem for computer networks. *International Journal of Computer Systems Science and Engineering*, 11(5):311–314, September 1996. CODEN CSSEEI. ISSN 0267-6192.

Hughes:1996:QCU

[HLMP96] R. J. Hughes, G. G. Luther, G. L. Morgan, and C. G. Peterson. Quantum cryptography over underground optical fibers. *Lecture Notes in Computer Science*, 1109: 329–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hohl:1993:SIH

[HLMW93] W. Hohl, X. Lai, T. Meier, and C. Waldvogel. Security of iterated hash functions based on block ciphers. In Stinson [Sti93b], pages 379–390. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). LCCN QA76.9.A25 C79 1993.

Hunter:1983:ERA

[HM83] D. G. N. Hunter and A. R. McKenzie. Experiments with relaxation algorithms for breaking simple substitution ciphers. *The Computer Journal*, 26(1):68–71, February 1983. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Hule:1988:RCW

[HM88] Harald Hule and Winfried B. Müller. On the RSA-cryptosystem with wrong keys. In *Contributions to general algebra, 6*, pages 103–109. Hölder-Pichler-Tempsky, Vienna, 1988.

Hafner:1991:COH

[HM91] Katie Hafner and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Simon and Schuster, 1230 Ave. of the Americas, New York, NY 10020, USA, 1991. ISBN 0-671-68322-5. 368 pp. LCCN QA76.9.A25 H34 1991. US$22.95. Interviews with some of the crackers who have appeared conspicuously in the press in the past few years. One of the co-authors is the New York Times reporter who broke the Stoll story to the public.

Hafner:1992:COH

[HM92] Katie Hafner and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Simon and Schuster, 1230 Ave. of the Americas, New York, NY 10020, USA, first Touchstone edition, 1992. ISBN 0-671-77879-X. 368 pp. LCCN QA76.9.A25 H28 1992.

Hafner:1995:COH

[HM95] Katie Hafner and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* Simon and Schuster, 1230 Ave. of the Americas, New York, NY 10020, USA, first Touchstone edition, 1995. ISBN 0-684-81862-0. 396 pp. LCCN QA76.9.A25 H28 1995.

Hedlund:1996:CFP

[HM96] Patric Hedlund and Gary Meyer. Computers, freedom, and privacy, 1996. 13 videocassettes (930 min.).

Harpes:1997:PC

[HM97a] C. Harpes and J. L. Massey. Partitioning cryptanalysis. *Lecture Notes in Computer Science*, 1267:13–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hoogeboom:1997:CPT

[HM97b] Hendrik Jan Hoogeboom and Anca Muscholl. The code problem for traces — improving the boundaries. *Theoretical Computer Science*, 172(1–2):309–321, February 10, 1997. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1997&volume=172&issue=1-2&aid=2419`.

Hoyle:1998:SKE

[HM98] Mark P. Hoyle and Chris J. Mitchell. On solutions to the key escrow problem. *Lecture Notes in Computer Science*, 1528: 277–306, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1528/15280277.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1528/15280277.pdf`.

Horster:1995:MRM

[HMP95] P. Horster, M. Michels, and H. Petersen. Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications. *Lecture Notes in Computer Science*, 917:224–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Harkavy:1998:IPP

[HMT+98] Michael Harkavy, Andrew Myers, J. D. Tygar, Alma Whitten, and H. Chi Wong. Invited presentations on Public Key Infrastructure. In USENIX [USE98b], page ?? ISBN 1-880446-97-9. LCCN

HF5004 .U74 1998. URL http://www.usenix.org/publications/library/proceedings/ec98/pki.html.

Harper:1993:PKC

[HMV93] Greg Harper, Alfred Menezes, and Scott A. Vanstone. Public-key cryptosystems with very small key lengths. *Lecture Notes in Computer Science*, 658:163–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580163.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580163.pdf.

Horvath:1994:PPM

[HMvT94] Tamás Horváth, Spyros S. Magliveras, and Tran van Trung. A parallel permutation multiplier for a PGM crypto-chip. In Desmedt [Des94b], pages 108–113. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390108.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390108.pdf.

Hennicker:1994:BAF

[HN94] R. Hennicker and F. Nickl. A behavioural algebraic framework for modular system design with reuse. *Lecture Notes in Computer Science*, 785:220–234, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Haastad:1998:SIR

[HN98] J. Håstad and M. Naslund. The security of individual RSA bits. In IEEE [IEE98a], pages 510–519. CODEN ASFPDV. ISBN 0-8186-9172-7 (softbound), 0-7803-5229-7 (casebound), 0-8186-9174-3 (microfiche). ISSN 0272-5428. LCCN QA267 .S95 1998 Sci-Eng. IEEE Catalog Number 98CB36280. IEEE Computer Society Press order number PR9172.

Hasegawa:1998:PIE

[HNM98] T. Hasegawa, J. Nakajima, and M. Matsui. A practical implementation of elliptic curve cryptosystems over GF(p) on a 16 bit microcomputer. *Lecture Notes in Computer Science*, 1431: 182–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Habutsu:1991:SKC

[HNSM91] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and

Shinsaku Mori. A secret key cryptosystem by iterating a chaotic map. *Lecture Notes in Computer Science*, 547:127–140, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hansmann:1999:SCA

[HNSS99] U. Hansmann, M. S. Nicklous, T. Schäck, and F. Seliger. *Smart Card Application Development Using Java*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-65829-7. 304 pp. US$49.95.

Hawkes:1996:ALC

[HO96] P. Hawkes and L. O'Connor. On applying linear cryptanalysis to IDEA. *Lecture Notes in Computer Science*, 1163:105–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hodges:1983:ATE

[Hod83] Andrew Hodges. *Alan Turing: the enigma*. Simon and Schuster, 1230 Ave. of the Americas, New York, NY 10020, USA, 1983. ISBN 0-671-49207-1, 0-09-152130-0 (Burnett Books). 587 pp. LCCN QA29.T8 H63 1983.

Hodges:1997:ATHa

[Hod97] A. Hodges. The Alan Turing home page. World-Wide Web site., 1997. URL `http://www.turing.org.uk/turing/`.

Hoffer:1955:MAC

[Hof55] Carol M. Hoffer. On the mathematical approach to cryptanalysis. Thesis, University of South Dakota, Vermillion, SD, USA, 1955. 65 pp.

Hoffman:1993:CC

[Hof93] Lance J. Hoffman. Clipping Clipper. *Communications of the Association for Computing Machinery*, 36(9):15–17, September 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/162691.html`.

Hoffman:1995:BBB

[Hof95] Lance J. Hoffman. *Building in big brother: the cryptographic policy debate*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 0-387-94441-9. xvi + 560 pp. LCCN QA76.9.A25 B85 1995.

Hofmeister:1999:ACA

[Hof99] T. Hofmeister. An application of codes to attribute-efficient learning. *Lecture Notes in Computer Science*, 1572:101–110, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hogan:1988:PIS

[Hog88] Carole B. Hogan. Protection imperfect: the security of some computing environments. *Operating Systems Review*, 22(3):7–27, July 1988. CODEN OSRED8. ISSN 0163-5980. See note [Wel88a].

Hollis:1987:TCA

[Hol87] J. B. Hollis. A technique for communicating AVL traffic by subliminal data signalling over a speech radio channel. In Muraszko [Mur87], pages 13/1–13/5. LCCN TE228 .C66 1987. Digest no.: 1987/21.

Holloway:1991:RA

[Hol91] Marguerite Holloway. R_x for addiction. *Scientific American*, 264(3):94–??, March 1991. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Honore:1919:STS

[Hon19] F. Honore. The secret telephone, are sound waves ever visible? *Scientific American*, 121(23):555, December 6, 1919. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v121/n23/pdf/scientificamerican12061919-555.pdf`.

Hontanon:1998:EC

[Hon98] Ramón J. Hontañón. Encryption 101 — the choices. *Sys Admin: The Journal for UNIX Systems Administrators*, 7(8):37–39, 40–44, August 1998. CODEN SYADE7. ISSN 1061-2688. URL `http://www.samag.com/`.

Hood:1980:EFS

[Hoo80] William Chester Hood. Encryption as a file security measure in large operating systems. Thesis (M.S.), University of Tennessee, Knoxville, Knoxville, TN, USA, 1980. iv + 116 pp.

Hoogendoorn:1982:SPK

[Hoo82] P. J. Hoogendoorn. On a secure public-key cryptosystem. In *Computational methods in number theory, Part I*, volume 154 of *Math. Centre Tracts*, pages 159–168. Math. Centrum, Amsterdam, 1982.

Han:1997:ICS

[HOQ97] Yongfei Han, Tatsuaki Okamoto, and Sihan Qing, editors. *Information and communications security: first international conference, ICICS '97, Beijing, China, November 11–13, 1997: proceedings*, volume 1334 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-63696-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I554 1997.

Horgan:1985:TIT

[Hor85] J. Horgan. Thwarting the information thieves: Fear of spying through simple or sophisticated electronics has spawned an industry whose challenge is to block the illegal interception of intelligence. *IEEE Spectrum*, 22(7):30–41, July 1985. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Horgan:1992:CSP

[Hor92] J. Horgan. Claude E. Shannon [profile]. *IEEE Spectrum*, 29(4):72–75, April 1992. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Horan:1994:CSO

[Hor94] William A. Horan. Computer security in open networks OSI to KERBEROS. Thesis (M.S.), State University of New York Institute of Technology at Utica/Rome, Utica, NY, USA, August 1994. 165 pp.

Horng:1995:PAU

[Hor95] Gwoboa Horng. Password authentication without using a password table. *Information Processing Letters*, 55(5):247–250, September 15, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Horng:1998:AAP

[Hor98] Gwoboa Horng. An active attack on protocols for server-aided RSA signature computation. *Information Processing Letters*, 65(2): 71–73, January 29, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Horster:1999:SSK

[Hor99] Patrick Horster. Von der Schwierigkeit, sichere Kryptosysteme zu entwerfen. (German) [The difficulty of designing safe cryptosystems]. In *Angewandte Mathematik, insbesondere Informatik*, pages 82–117. Vieweg & Son, Braunschweig, Germany, 1999.

Herzberg:1987:PPS

[HP87] Amir Herzberg and Shlomit S. Pinter. Public protection of software. *ACM Transactions on Computer Systems*, 5(4):371–393, November 1987. CODEN ACSYEC. ISSN 0734-2071. URL `http://www.acm.org:80/pubs/citations/journals/tocs/1987-5-4/p371-herzberg/`.

Hung:1994:FRD

[HP94] Ching Yu Hung and Behrooz Parhami. Fast RNS division algorithms for fixed divisors with application to RSA encryption. *Information Processing Letters*, 51(4): 163–169, August 24, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Handschuh:1998:SCC

[HP98a] Helena Handschuh and Pascal Paillier. Smart card crypto-coprocessors for public-key cryptography. *CryptoBytes*, 4(1):6–11, Summer 1998. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto4n1.pdf`.

Horn:1998:APF

[HP98b] G. Horn and B. Preneel. Authentication and payment in future mobile systems. *Lecture Notes in Computer Science*, 1485: 277–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Handschuh:1999:SDK

[HP99a] H. Handschuh and B. Preneel. On the security of double and 2-key triple modes of operation. *Lecture Notes in Computer Science*, 1636: 215–230, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Handschuh:1999:SDT

[HP99b] H. Handschuh and B. Preneel. On the security of double and 2-key triple modes of operation. In Knudsen [Knu99c], pages 215–230. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Heileman:1999:IWC

[HPA99] G. L. Heileman, C. E. Pizano, and C. T. Abdallah. Image watermarking for copyright protections. *Lecture Notes in Computer Science*, 1619: 226–245, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hernandez:1998:SML

[HPG98] Juan Ramón Hernández and Fernando Pérez-González. Shedding more light on image watermarks. *Lecture*

Notes in Computer Science, 1525:191–207, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250191.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250191.pdf.

Hoffstein:1998:NRB

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: a ring-based public key cryptosystem. *Lecture Notes in Computer Science*, 1423:267–288, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1423/14230267.htm; http://link.springer-ny.com/link/service/series/0558/papers/1423/14230267.pdf.

Holland:1982:GSA

[HR82] Edward R. Holland and James L. Robertson. GUEST — a signature analysis based test system for ECL logic. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 33(3):26–29, March 1982. CODEN HPJOAX. ISSN 0018-1153.

Hwang:1990:PKA

[HR90] Tzonelih Hwang and T. R. N. Rao. Private-key algebraic-code cryptosystems with high information rates. *Lecture Notes in Computer Science*, 434:657–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340657.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340657.pdf.

Hollander:1996:KWS

[HRT96] Isaac Hollander, P. Rajaram, and Constantin Tanno. Kerberos on Wall Street. In USENIX [USE96e], pages 105–112. ISBN 1-880446-79-0. LCCN QA76.9.A25 U83 1996. URL http://www.usenix.org/publications/library/proceedings/sec96/hollander.html.

Harrison:1976:POS

[HRU76] Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in operating systems. *Communications of the Association for Computing Machinery*, 19(8):461–471, August 1976. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Hruby:1995:QDQ

[Hru95a] J. Hruby. Q-deformed quantum cryptography. *Lecture Notes in Computer Science*, 950:468–472, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500468.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500468.pdf.

Hruby:1995:QQC

[Hru95b] J. Hruby. Q-deformed quantum cryptography. *Lecture Notes in Computer Science*, 950:468–472, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hruby:1996:SCI

[Hru96] J. Hruby. Smart card with interferometric quantum cryptography device. *Lecture Notes in Computer Science*, 1029:282–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hruby:1998:TQC

[Hru98] J. Hruby. Trends in quantum cryptography in Czech Republic. *Lecture Notes in Computer Science*, 1438:261–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hruby:1999:SUD

[Hru99] P. Hruby. Structuring UML design deliverables. *Lecture Notes in Computer Science*, 1618:278–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hernandez:1999:CLM

[HRVV99] V. Hernandez, J. E. Roman, A. M. Vidal, and V. Vidal. Calculation of lambda modes of a nuclear reactor: a parallel implementation using the implicitly restarted Arnoldi method. *Lecture Notes in Computer Science*, 1573:43–57, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Haastad:1985:CST

[HS85] J. Håstad and A. Shamir. The cryptographic security of truncated linearly related variables. In ACM [ACM85], pages 356–362. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6 A13 1985. URL http://www.acm.org/pubs/articles/proceedings/stoc/22145/p356-hastad/p356-hastad.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/22145/p356-hastad/. ACM order no. 508850.

Hammer:1987:EUH

[HS87] Joseph Hammer and Dinesh G. Sarvate. Encryption using Hungarian rings. *Discrete Applied Mathematics*, 16(2):151–155, 1987. CODEN DAMADU. ISSN 0166-218X.

Hardjono:1989:TCB

[HS89] Thomas Hardjono and Jennifer Seberry. *Towards the cryptanalysis of Bahasa Indonesia and Malaysia*, volume 2 of *CCSR Tutorial Series in Computer Security*. Centre for Commuter Security Research, Canberra, Australia, 1989. ISBN 0-7317-0091-0. vi + 148 pp. LCCN ????

Hardjono:1990:SKS

[HS90] Thomas Hardjono and Jennifer Seberry. Search key substitution in the encipherment of B-trees. In McLeod et al. [MSDS90], pages 50–58. ISBN 1-55860-149-X. LCCN QA76.9.D3I559 1990. URL `http://www.vldb.org/dblp/db/conf/vldb/HardjonoS90.html`.

Haber:1991:HTD

[HS91] Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3 (2):99–111, 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Hinsley:1993:CIS

[HS93] Sir F. H. Hinsley and Alan Stripp, editors. *Codebreakers: the inside story of Bletchley Park*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1993. ISBN 0-19-820327-6, 0-19-285304-X. xxi + 321 pp. LCCN D810.C88 M46 1993.

Hardjono:1994:AMS

[HS94] T. Hardjono and J. Seberry. Authentication via multi-service tickets in the Kuperee server. *Lecture Notes in Computer Science*, 875:143–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Handel:1996:HDO

[HS96a] T. G. Handel and M. T. Sandford. Hiding data in the OSI network model. In Anderson [And96c], pages 23–38. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054222.html`.

Hardjono:1996:RKA

[HS96b] T. Hardjono and J. Seberry. Replicating the Kuperee authentication server for increased security and reliability. *Lecture Notes in Computer Science*, 1172: 14–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hall:1997:REG

[HS97] C. Hall and B. Schneier. Remote electronic gambling. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1997. URL `http://www.counterpane.com/remote_electronic_gambling.html`. Also published in *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 227–230.

Helme:1997:SFF

[HSK97] Arne Helme and Tage Stabell-Kulø. Security functions for a file repository. *Operating Systems Review*, 31(2):3–8, April 1997. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Harasawa:1999:CMF

[HSSI99] R. Harasawa, J. Shikata, J. Suzuki, and H. Imai. Comparing the MOV and FR reductions in elliptic curve cryptography. *Lecture Notes in Computer Science*, 1592:190–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hornauer:1994:MCA

[HSW94] G. Hornauer, W. Stephan, and R. Wernsdorf. Markov ciphers and alternating groups. *Lecture Notes in Computer Science*, 765: 453–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hauser:1996:MBI

[HSW96] R. Hauser, M. Steiner, and M. Waidner. Micropayments based on iKP. ????, January 1996. URL `http://www.zurich.ibm.com:80/Technology/Security/extern/ecommerce/iKP.html`.

Hinsley:1979:BISa

[HT79] F. H. (Francis Harry) Hinsley and E. E. Thomas. *British intelligence in the Second World War: its influence on strategy and operations.* London, UK, 1979. various pp. UK£10.00 (vol. 1). Vol. 3, pt. 2 has additional author C. A. G. Simkins.

Heys:1995:ACS

[HT95] H. M. Heys and S. E. Tavares. Avalanche characteristics of substitution-permutation encryption networks. *IEEE Transactions on Computers*, 44(9):1131–1139, September 1995. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=464391.

Hada:1998:EZP

[HT98] S. Hada and T. Tanaka. On the existence of 3-Round zero-knowledge protocols. *Lecture Notes in Computer Science*, 1462:408–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hada:1999:RBO

[HT99] S. Hada and T. Tanaka. A relationship between one-wayness and correlation intractability. *Lecture Notes in Computer Science*, 1560: 82–96, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Handschuh:1999:DOE

[HTY99] H. Handschuh, Y. Tsiounis, and M. Yung. Decision oracles are equivalent to matching oracles. *Lecture Notes in Computer Science*, 1560:276–289, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Huang:1988:APE

[Hua88] Min Qiang Huang. An attack to Pless' encryption scheme. *Kexue Tongbao (English Ed.)*, 33(11):885–889, 1988. ISSN 0250-7862.

Huber:1991:SCC

[Hub91] Klaus Huber. Some considerations concerning the selection of RSA moduli. *Lecture Notes in Computer Science*, 547:294–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470294.htm; http://link.springer-ny.com/link/service/series/0558/papers/0547/05470294.pdf.

Huber:1998:MAE

[Hub98] Klaus Huber. MAGENTA: Advanced Encryption Standard candidate. In National Institute of Standards and Technology [Nat98], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/round1.htm#algtable. No slides or paper for the conference talk are available.

Hulme:1898:CHP

[Hul98] F. Edward (Frederick Edward) Hulme. *Cryptography; or, The history, principles, and practice of cipher-writing*. Ward, Lock and Co., Limited, ????, 1898. 192 pp. LCCN Z 104 H91. First edition. Galland, p. 94. Bound in yellow cloth; stamped in black. Library of the American Cryptogram Association (George C. Lamb Collection).

Hunter:1985:ARK

[Hun85] D. G. N. Hunter. Algorithm 121: RSA key calculation in Ada. *The Computer Journal*, 28(3):343–348, July 1985. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/28/3/343.full.pdf+html; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/343.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/344.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/345.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/346.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/347.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_28/Issue_03/tiff/348.tif. See note [Wic87].

Hurwicz:1998:CTM

[Hur98] Michael Hurwicz. Cracker tracking: Tighter security with intrusion detection. *BYTE Magazine*, 23(5): 112C, 112D, 112F, 112H, 112J, May 1998. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Husain:1994:EI

[Hus94] Kamran Husain. Extending Imake. *Dr. Dobb's Journal of Software Tools*, 19(6):70, 72, 74–76, June 1994. CODEN DDJOEB. ISSN 1044-789X.

Husemann:1999:SCD

[Hus99] Dirk Husemann. The smart card: Don't leave home without it. *IEEE Concurrency*, 7(2):24–27, April/June 1999. CODEN IECMFX. ISSN 1092-3063 (print), 1558-0849 (electronic). URL http://dlib.computer.org/pd/books/pd1999/pdf/p2024.pdf; http://www.computer.org/concurrency/pd1999/p2024abs.htm.

Hulaas:1998:MLI

[HVH98] J. Hulaas, A. Villazon, and J. Harms. A multi-level interface structure for the selective publication of services in an open environment. *Lecture Notes in Computer Science*, 1543: 293–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hardy:1975:ITN

[HW75] Godfrey H. Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, UK, fourth edition, 1975. ISBN 0-19-853310-7 (invalid checksum??). 421 pp. LCCN ????

Hartnell:1976:PFM

[HW76] B. L. Hartnell and H. C. Williams, editors. *Proceedings of the Fifth Manitoba Conference on Numerical Mathematics, October 1–4, 1975*, volume 16 of *Congressus Numerantium*. Utilitas Mathematica Publishers, Winnipeg, MN, Canada, 1976.

Hardy:1979:ITN

[HW79] G. H. (Godfrey Harold) Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. Clarendon Press, Oxford, UK, fifth edition, 1979. ISBN 0-19-853170-2, 0-19-853171-0 (paperback). xvi + 426 pp. LCCN QA241 .H28 1979.

Huthnance:1988:UPP

[HW88] E. Dennis Huthnance and Joe Warndof. On using primes for public key encryption systems. *Applied Mathematics Letters*, 1(3): 225–227, 1988. CODEN AMLEEL. ISSN 0893-9659.

Hotchkiss:1991:ASI

[HW91] R. S. Hotchkiss and C. L. Wampler. The auditorialization of scientific information. In IEEE [IEE91], pages 453–461. ISBN 0-8186-9158-1 (IEEE case), 0-8186-2158-3 (IEEE paper), 0-8186-6158-5 (IEEE microfiche), 0-89791-459-7 (ACM). LCCN QA76.5 .S894 1991. ACM order number 415913. IEEE Computer Society Press order number 2158. IEEE catalog number 91CH3058-5.

Hsu:1997:DWV

[HW97] Chiou-Ting Hsu and Ja-Ling Wu. Digital watermarking for video. In IEEE [IEE97c], pages 217–219. ISBN 0-7803-4137-6 (softbound), 0-7803-4138-4 (microfiche), 0-7803-4139-2 (CDROM). LCCN TK5102.5.D448245 1997. Two volumes. IEEE catalog number 97TH8306.

Hsu:1998:DBW

[HW98a] Chiou-Ting Hsu and Ja-Ling Wu. DCT-based watermarking for video. *IEEE Transactions on Consumer Electronics*, 44(1):206–216, February 1998. CODEN ITCEDA. ISSN 0098-3063.

Hsu:1998:MWD

[HW98b] Chiou-Ting Hsu and Ja-Ling Wu. Multiresolution watermarking for digital images. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 45(8):1097–1101, August 1998. CODEN ICSPE5. ISSN 1057-7130 (print), 1558-125X (electronic).

Hwang:1998:AUS

[HW98c] Tzonelih Hwang and Chih-Hung Wang. Arbitrated unconditionally secure authentication scheme with multi-senders. *Information Processing Letters*, 65(4): 189–193, February 27, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:1991:CGO

[Hwa91] Tzonelih Hwang. Cryptosystem for group oriented cryptography. *Lecture Notes in Computer Science*, 473:352–360, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hwang:1992:AOT

[Hwa92a] Tzonelih Hwang. Attacks on Okamoto and Tanaka's one-way ID-based key distribution system. *Information Processing Letters*, 43 (2):83–86, August 24, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:1992:EIB

[Hwa92b] Tzonelih Hwang. Efficient ID-based key distribution with tamperfree devices. *Information Processing Letters*, 44(1):31–34, November 9, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:1992:EIK

[Hwa92c] Tzonelih Hwang. Efficient ID-based key distribution with tamperfree devices. *Information Processing Letters*, 44(1):31–34, November 09, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:1992:PGO

[Hwa92d] Tzonelih Hwang. Protocols for group oriented secret sharing. *Information Processing Letters*, 42(4):179–182, June 19, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:1993:SSD

[Hwa93] Tzonelih Hwang. Scheme for secure digital mobile communications based on symmetric key cryptography. *Information Processing Letters*, 48(1):35–37, October 29, 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hwang:1997:CKA

[Hwa97] M.-S. Hwang. A cryptographic key assignment scheme in a hierarchy for access control. *Mathematical and computer modelling*, 26(2):27–??, ???? 1997. CODEN MCMOEG. ISSN 0895-7177 (print), 1872-9479 (electronic).

Hasan:1993:MMO

[HWB93] M. A. Hasan, M. Z. Wang, and V. K. Bhargava. A modified Massey–Omura parallel multiplier for a class of finite field. *IEEE Transactions on Computers*, 42(10):1278–1280, October 1993. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

He:1996:TLR

[HWF96] Ye Ping He, Wei Wang, and Shu Xiang Fan. A two-level refined design of an RSA public key cryptosystem. *J. Lanzhou Univ. Nat. Sci.*, 32 (2):10–13, 1996. CODEN LCTHAF. ISSN 0455-2059.

Hong:1998:FIE

[HWJ98] L. Hong, Y. Wan, and A. Jain. Fingerprint image enhancement: Algorithm and performance evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(8):777–789, August 1998. CODEN ITPIDJ. ISSN 0162-8828. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073136.html`.

Hall:1998:BPPa

[HWKS98a] C. Hall, D. Wagner, J. Kelsey, and B. Schneier. Building PRFs from PRPs. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. URL `http://www.counterpane.com/prf-prp.html`. PRF is pseudo-random function, and PRP is pseudo-random permutation.

Hall:1998:BPPb

[HWKS98b] C. Hall, D. Wagner, J. Kelsey, and B. Schneier. Building PRFs from PRPs. *Lecture Notes in Computer Science*, 1462:370–389, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). PRF is pseudo-random function, and PRP is pseudo-random permutation.

Hohl:1994:SIH

[HXMW94] Walter Hohl, Lai Xuejia, Thomas Meier, and Christian Waldvogel. Security of iterated hash functions based on block ciphers. *Lecture Notes in Computer Science*, 773:379–390, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Harn:1993:GUS

[HY93a] L. Harn and S. Yang. Group-oriented undeniable signature schemes without the assistance of a mutually trusted party. *Lecture Notes in Computer Science*, 718:133–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Harn:1993:PKC

[HY93b] L. Harn and S. Yang. Public-key cryptosystem based on the discrete logarithm problem. *Lecture Notes in Computer Science*, 718:469–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hwang:1995:TPE

[HY95] Min-Shiang Hwang and Wei-Pang Yang. A two-phase encryption scheme for enhancing database security. *The Journal of Systems and Software*, 31(3): 257–265, December 1995. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Hirose:1998:ADK

[HY98a] S. Hirose and S. Yoshida. An authenticated Diffie–Hellman key agreement protocol secure against active attacks. *Lecture Notes in Computer Science*, 1431: 135–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hirose:1998:ADH

[HY98b] Shouichi Hirose and Susumu Yoshida. An authenticated Diffie–Hellman key agreement protocol secure against active attacks. *Lecture Notes in Computer Science*, 1431: 135–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310135.htm; http://link.springer-ny.com/link/service/series/0558/papers/1431/14310135.pdf`.

Hsieh:1998:H

[HYHW98] Tsu-Miin Hsieh, Yi-Shiung Yeh, Yung-Cheng Hsieh, and Chan-Chi Wang. A homophonic DES. *Information Processing Letters*, 66 (6):317–320, June 30, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hsieh:1999:OWH

[HYLT99] T.-M. Hsieh, Y.-S. Yeh, C.-H. Lin, and S.-H. Tuan. One-way hash functions with changeable parameters. *Information Sciences*, 118(1):223–239, September

1999. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Hardjono:1993:PDM

[HZ93] T. Hardjono and Y. Zheng. A practical digital multisignature scheme based on discrete logarithms. *Lecture Notes in Computer Science*, 718:122–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ibbotson:1997:CPI

[Ibb97] J. Ibbotson. Copyright protection in images in the digital environment. *The Journal of audiovisual media in medicine*, 20(1):15–??, ???? 1997. ISSN 0140-511X.

Anonymous:1993:CCA

[IBM93] IBM. *Common Cryptographic Architecture: Cryptographic Application Programming Interface — Public Key Algorithm*. IBM Corporation, San Jose, CA, USA, April 1993. ?? pp. IBM publication SC40-1676.

IBM:19xx:PSP

[IBMxx] IBM Research. The proactive security project. Technical report, IBM, ??, Israel, 19xx. ?? pp. URL `http://www.ibm.net.il/ibm_il/int-lab/Proactive/home.html`.

IEEE:1974:ASS

[IEE74] IEEE, editor. *15th Annual Symposium on Switching and Automata Theory, October 14–16, 1974, the University of New Orleans*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1974.

IEEE:1979:ASF

[IEE79] IEEE, editor. *20th Annual Symposium on Foundations of Computer Science: Oct. 29–31, 1979, San Juan, Puerto Rico*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1979. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA267 .S95 1979; TK7885.A1 S92 1979.

IEEE:1980:PSS

[IEE80] IEEE, editor. *Proceedings of the 1980 Symposium on Security and Privacy, April 14–16, 1980 Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1980. LCCN QA76.9.A25S95 1980.

IEEE:1981:CLC

[IEE81] IEEE, editor. *6th Conference on Local Computer*

Networks, Hilton Inn, Minneapolis, Minnesota, October 12–14, 1981. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1981. CODEN CLCPDN. LCCN TK 5105.5 C66 1981. IEEE catalog no. 81CH1690-7.

IEEE:1982:ASF

[IEE82a] IEEE, editor. *23rd annual Symposium on Foundations of Computer Science, November 3–5, 1982, Chicago, Illinois*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

IEEE:1982:CFP

[IEE82b] IEEE, editor. *COMPCON Fall '82: Proceedings of the 25th International Conference of the Institute of Electrical and Electronics Engineers Computer Society, Capitol Hilton Hotel, Washington, DC, 1982*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982. ISBN ???? LCCN QA76.5 I578 1982. IEEE catalog no. 82CH1796-2.

IEEE:1983:PSS

[IEE83] IEEE, editor. *Proceedings of the 1983 Symposium on Security and Privacy, April 25–27, 1983, Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1983. ISBN 0-8186-0467-0 (paperback), 0-8186-4467-2 (microfiche), 0-8186-8467-4 (hardcover). LCCN QA76.9.A25 S95 1983.

IEEE:1984:ASF

[IEE84] IEEE, editor. *25th annual Symposium on Foundations of Computer Science, October 24–26, 1984, Singer Island, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1984. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog no. 84CH2085-9.

IEEE:1985:FOC

[IEE85] IEEE, editor. *26th annual Symposium on Foundations of Computer Science, October 21–23, 1985, Portland, OR*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985. ISBN 0-8186-0644-4 (paperback), 0-8186-

4644-6 (microfiche), 0-8186-8644-8 (hardcover). LCCN QA 76 S979 1985.

IEE:1986:CEC

[IEE86a] IEE. *Colloquium on "Encryption for Cable and DBS": Wednesday, 19 February 1986*, volume 1986/24. Institution of Electrical Engineers, London, UK, 1986. various pp.

IEEE:1986:ASF

[IEE86b] IEEE, editor. *27th annual Symposium on Foundations of Computer Science, October 27–29, 1986, Toronto, ON, Canada*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1986. ISBN 0-8186-0740-8 (paperback), 0-8186-4740-X (microfiche), 0-8186-8740-1 (casebound). LCCN QA 76 S979 1986; TK7885.A1 S92 1986.

IEEE:1987:ASF

[IEE87a] IEEE, editor. *28th annual Symposium on Foundations of Computer Science, October 12–14, 1987, Los Angeles, CA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. ISBN 0-8186-0807-2, 0-8186-4807-4 (fiche), 0-8186-8807-6 (case). LCCN QA 76 S979 1987.

IEEE:1987:IIG

[IEE87b] IEEE, editor. *IEEE/IEICE Global Telecommunications Conference: conference record, Nov. 15–18, 1987, Tokyo, Japan [GLOBECOM Tokyo '87]*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. Three volumes. IEEE catalog no. 87CH2520-5.

IEEE:1987:PIS

[IEE87c] IEEE, editor. *Proceedings / 1987 IEEE Symposium on Security and Privacy, April 27–29, 1987, Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. ISBN 0-8186-8771-1 (hardback), 0-8186-0771-8 (paperback), 0-8186-4771-X (microfiche). LCCN QA 76.9 A25 I43 1987. IEEE catalog number 87CH2416-6. Computer Society Order Number 771.

IEEE:1988:FAC

[IEE88] IEEE, editor. *Fourth Aerospace Computer Security Applications Conference, Orlando, FL, USA, December 12–16, 1988*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-0895-

1. LCCN TL787 .A471 1988; QA76.9.A25 A39 1988. IEEE catalog number 88CH2629-5. IEEE Computer Society order number 895.

IEEE:1989:ASF

[IEE89] IEEE, editor. *30th annual Symposium on Foundations of Computer Science, October 30–November 1, 1989, Research Triangle Park, NC*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. CODEN ASFPDV. ISBN 0-8186-1982-1 (casebound), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1989. IEEE catalog number 89CH2808-4.

IEEE:1991:PSA

[IEE91] IEEE, editor. *Proceedings, Supercomputing '91: Albuquerque, New Mexico, November 18–22, 1991*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. ISBN 0-8186-9158-1 (IEEE case), 0-8186-2158-3 (IEEE paper), 0-8186-6158-5 (IEEE microfiche), 0-89791-459-7 (ACM). LCCN QA76.5 .S894 1991. ACM order number 415913. IEEE Computer Society Press order number 2158. IEEE catalog number 91CH3058-5.

IEEE:1992:CSF

[IEE92a] IEEE, editor. *The Computer Security Foundations Workshop V proceedings: June 16–18, 1992, the Franconia Inn, Franconia, New Hampshire*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-8186-2850-2. LCCN QA 76.9 A25 C655 1992. IEEE catalog number 92TH0447-3.

IEEE:1992:PEA

[IEE92b] IEEE, editor. *Proceedings / Eighth Annual Computer Security Applications Conference, San Antonio, Texas, November 30–December 4, 1992*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-8186-3115-5 (paperback), 0-8186-3116-3 (microfiche), 0-8186-3117-1 (casebound). LCCN QA76.9.A25 C6375 1992. IEEE Computer Society Press order number 3115. IEEE catalog number 92TH04070-5.

IEEE:1992:PIC

[IEE92c] IEEE, editor. *Proceedings: 1992 IEEE Computer Society Symposium on Research in Security and Privacy, May 4–6, 1992, Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-8186-2825-1 (paperback) 0-8186-2826-X (microfiche) 0-8186-2827-8 (casebound). LCCN QA 76.9 A25 I34 1992. IEEE Catalog Number 92CH3157-5. IEEE Computer Society Press order number 2825.

IEEE:1992:PII

[IEE92d] IEEE, editor. *Proceedings: IEEE Infocom '92, the conference on computer communications, one world through communications, eleventh annual joint conference of the IEEE Computer and Communications Societies, Florence, Italy*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. Three volumes. IEEE Computer Society order number 2860. IEEE catalog number 92CH3133-6.

IEEE:1993:FIW

[IEE93a] IEEE, editor. *Fourth IEEE Workshop on Workstation Operating Systems (WWOS-IV), October 14–15, 1993, Napa, CA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1993. ISBN 0-8186-4000-6 (paper), 0-8186-4001-4 (microfiche). LCCN QA76.76.O63 W667 1993. IEEE catalog number 93TH0553-8.

IEEE:1993:ICS

[IEE93b] IEEE, editor. *IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California, 24–26 May, 1993*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1993. ISBN 0-8186-3370-0 (paperback), 0-8186-3371-9 (microfiche), 0-8186-3372-7 (casebound). LCCN QA 76.9 A25 I34 1993. IEEE catalog number 93CH3290-4.

IEEE:1993:PNA

[IEE93c] IEEE, editor. *Proceedings, Ninth Annual Computer Security Applications Conference, December 6–10, 1993, Orlando, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1993. ISBN 0-8186-4330-7. ISSN 1063-9527. LCCN QA76.9.A25 C6375 1993. IEEE Computer Society Press order number 4330-02. IEEE catalog number 93TH0581-9.

IEEE:1994:IIW

[IEE94a] IEEE, editor. *1994 IEEE-IMS Workshop on Information Theory and Statistics: October 27–29, 1994, Holiday Inn Old Town, Alexan-*

dria, Virginia. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-7803-2761-6. LCCN QA276 .I54 1994. IEEE Catalog No. 94TH8100.

IEEE:1994:CPN

[IEE94b] IEEE, editor. *COMPASS '94: proceedings of the Ninth Annual Conference on Computer Assurance: June 27–July 1, 1994, National Institute of Standards and Technology, Gaithersburg, MD: safety, reliability, fault tolerance, concurrency and real time security*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-7803-1856-0 (casebound), 0-7803-1855-2 (softbound), 0-7803-1857-9 (microfiche). LCCN QA 76.76 R44 C668 1994. IEEE catalog number 94CH3415-7.

IEEE:1994:PAC

[IEE94c] IEEE, editor. *Proceedings / 10th Annual Computer Security Applications Conference, December 5–9, 1994, Orlando, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-6795-8 (paperback), 0-8186-6796-6 (microfiche). LCCN QA76.9.A25 C6375.

IEEE:1994:PIC

[IEE94d] IEEE, editor. *Proceedings: 1994 IEEE Computer Society Symposium on Research in Security and Privacy, May 16–18, 1994, Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-5675-1 (paperback), 0-8186-5676-X (microfiche) 0-8186-5677-8 (case). LCCN QA 76.9 A25 I34 1994. IEEE Catalog Number 94CH3444-7.

IEEE:1994:PSH

[IEE94e] IEEE, editor. *Proceedings of the Scalable High-Performance Computing Conference, May 23–25, 1994, Knoxville, Tennessee*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-5680-8, 0-8186-5681-6. LCCN QA76.5 .S244 1994. IEEE catalog number 94TH0637-9.

IEEE:1994:TAJ

[IEE94f] IEEE, editor. *Thirteenth Annual Joint Conference of the IEEE Computer and Communications Societies, 14–16 June 1994, Toronto, Canada (IEEE Infocom '94)*. IEEE Computer Society Press, 1109

Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-5571-2 (microfiche). LCCN ???? Three volumes. IEEE Computer Society Press Order Number 5570-02. IEEE Catalog Number 94CH3401-7.

IEE:1995:PIC

[IEE95a] IEE, editor. *Proceedings of the 5th International Conference on Image Processing and its Applications, Edinburgh, UK, July 4–6 1995*, volume 410 of *IEE conference publication*. IEE, London, UK, 1995. ISBN 0-85296-642-3. LCCN ????

IEEE:1995:PIS

[IEE95b] IEEE, editor. *Proceedings: 1995 IEEE Symposium on Security and Privacy, May 8–10, 1995, Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1995. ISBN 0-7803-2540-0, 0-8186-7015-0, 0-7803-2541-9. LCCN QA 76.9 A25 I43 1995. IEEE Catalog Number 95CH35760.

IEEE:1995:PII

[IEE95c] IEEE, editor. *Proceedings: IEEE INFOCOM '95, the conference on computer communications: fourteenth annual Joint Conference of the IEEE Computer and Communications Societies: bringing information to people: April 2-6, 1995, Boston, Massachusetts*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, April 1995. ISBN 0-7803-2525-7 (microfiche). ISSN 0743-166X. LCCN TK 5105.5 I33 1995. Three volumes. IEEE catalog number 95CH35759. IEEE Computer Society Press order number PR06990.

IEEE:1996:ASF

[IEE96a] IEEE, editor. *37th Annual Symposium on Foundations of Computer Science: October 14–16, 1996, Burlington, Vermont*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. CODEN ASFPDV. ISBN 0-7803-3762-X (casebound), 0-8186-7594-2 (softbound), 0-8186-7596-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1996. IEEE catalog number 96CH35973. IEEE Computer Society Press order number PR07594.

IEEE:1996:IIC

[IEE96b] IEEE, editor. *IEEE International Conference on Multimedia Computing and Systems, Hiroshima, Japan, 17–23 June, 1996*. IEEE Computer Society Press, 1109 Spring Street, Suite

300, Silver Spring, MD 20910, USA, 1996. ISBN 0-8186-7436-9 (paperback), 0-8186-7438-5, 0-8186-7437-7 (microfiche). LCCN QA76.575.I623 1996. IEEE Computer Society Press order number PR07436. IEEE Order Plan catalog number 96TB100057.

IEEE:1996:PICb

[IEE96c] IEEE, editor. *Proceedings / 9th IEEE Computer Security Foundations Workshop, June 10–12, 1996, Dromquinna Manor, Kenmare, County Kerry, Ireland*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN 0-8186-7522-5. LCCN QA 76.9 A25 C655 1996. IEEE catalog number 96TB100047.

IEEE:1996:PIH

[IEE96d] IEEE, editor. *Proceedings, IEEE High-Assurance Systems Engineering Workshop, October 21–22, 1996, Niagara on the Lake, Ontario, Canada*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN 0-8186-7629-9 (paperback), 0-8186-7631-0 (microfiche). LCCN TA168.I199 1997. IEEE Computer Society Press Order Number PR07629. IEEE Order Plan Catalog Number 96TB100076.

IEEE:1996:PICa

[IEE96e] IEEE, editor. *Proceedings, International Conference on Image Processing: September 16–19, 1996, Lausanne, Switzerland (ICIP '96)*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN 0-7803-3258-X (softbound), 0-7803-3259-8 (casebound), 0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM). LCCN TK8315.I222 1996. Three volumes. IEEE catalog number 96CH35919.

IEEE:1996:SCR

[IEE96f] IEEE, editor. *Southcon/96 conference record: Orange County Convention Center, Orlando, Florida, June 25–27, 1996*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. CODEN SCOREX. ISBN 0-7803-3268-7 (softbound), 0-7803-3269-5 (casebound). LCCN TK 7801 S68 1996. IEEE catalog number 96CB35925.

IEE:1997:SIC

[IEE97a] IEE, editor. *Sixth International Conference on Image Processing and its Applications: 14–17 July, 1997,* *Trinity College, Dublin, Ireland*, volume 443 of *Conference publication (Institute of Electrical Engineers)*. IEE, London, UK, 1997. ISBN 0-85296-692-X. LCCN TK5.I4 no.443; TA1632 .I553 1997. Two volumes.

IEEE:1997:ACS

[IEE97b] IEEE, editor. *13th Annual Computer Security Applications Conference, San Diego, California, December 8–12, 1997: proceedings (ACSAC'97)*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. ISBN 0-8186-8274-4 (paperback), 0-8186-8275-2 (casebound), 0-8186-8276-0 (microfiche). LCCN QA76.9.A25 C6375 1997. IEEE Computer Society Press order number PR08274. IEEE order plan catalog number 97TB100213.

IEEE:1997:ICD

[IEE97c] IEEE, editor. *1997 13th International Conference on Digital Signal Processing: DSP 97: July 2–4, 1997: Conference Centre "P. M. Nomikos", Santorini, Hellas (Greece)*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. ISBN 0-7803-4137-6 (softbound), 0-7803-4138-4 (microfiche), 0-7803-4139-2 (CDROM). LCCN TK5102.5.D448245 1997. Two volumes. IEEE catalog number 97TH8306.

IEEE:1997:IICb

[IEE97d] IEEE, editor. *1997 IEEE International Conference on Acoustics, Speech, and Signal Processing: April 21–24, 1997, Munich, Germany*, Proceedings of the International Conference on Acoustics, Speech, and Signal Processing. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. CODEN IPRODJ. ISBN 0-8186-7920-4 (casebound), 0-8186-7919-0, 0-8186-7921-2 (microfiche). ISSN 0736-7791. LCCN TK 7882 S65 I16 1997. Five volumes. IEEE catalog number 97CB36052. IEEE Computer Society Press order number PR07919.

IEEE:1997:IWS

[IEE97e] IEEE, editor. *1997 IEEE Workshop on Speech Coding for Telecommunications proceedings: back to basics — attacking fundamental problems in speech coding, Pocono Manor Inn, Pocono Manor, Pennsylvania, USA, September 7–10, 1997*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver

Spring, MD 20910, USA, 1997. ISBN 0-7803-4073-6 (softbound), 0-7803-4074-4 (microfiche). LCCN TK7882.S65I43 1997. IEEE catalog number 97TH8295.

IEEE:1997:ASF

[IEE97f] IEEE, editor. *38th Annual Symposium on Foundations of Computer Science: October 20–22, 1997, Miami Beach, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. CODEN ASFPDV. ISBN 0-8186-8197-7 (paperback), 0-8186-8198-5 (casebound), 0-8186-8199-3 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 .S92 1997. IEEE catalog number 97CB36150. IEEE Computer Society Press order number PR08197.

IEEE:1997:IICa

[IEE97g] IEEE, editor. *IEEE International Conference on Consumer Electronics, Rosemont, IL, USA, June 11–13, 1997*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. CODEN DTPEEL. ISBN 0-7803-3735-2 (casebound), 0-7803-3734-4 (paperback), 0-7803-3736-0 (microfiche). ISSN 0747-668X. LCCN ????

IEEE:1997:ICI

[IEE97h] IEEE, editor. *International Conference on Image Processing: October 26–29, 1997, Santa Barbara, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. ISBN 0-8186-8183-7, 0-8186-8184-5 (case). LCCN TK8315 .I16 1997. Three volumes. IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144.

IEEE:1997:PIS

[IEE97i] IEEE, editor. *Proceedings / 1997 IEEE Symposium on Security and Privacy, May 4–7, 1997, Oakland, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. ISBN 0-8186-7828-3 (softbound), 0-7803-4159-7 (casebound), 0-8186-7830-5 (microfiche). LCCN QA 76.9 A25 I43 1997.

IEEE:1997:PICa

[IEE97j] IEEE, editor. *Proceedings, International Conference on Image Processing: October 26–29, 1997, Santa Barbara, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. ISBN 0-8186-8183-7 (paperback), 0-8186-8184-5 (casebound), 0-8186-8185-3 (microfiche). LCCN TK8315 .I16 1997. Three volumes. IEEE order plan catalog number 97CB36144.

IEEE:1997:PICb

[IEE97k] IEEE, editor. *Proceedings of 1997 International Conference on Information, Communications, and Signal Processing, 9–12 September 1997, Singapore: theme: Trends in information systems engineering and wireless multimedia communications*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. ISBN 0-7803-3676-3 (softbound,) 0-7803-3677-1 (microfiche). LCCN TK5102.9.I546 1997. Three volumes. IEEE catalog number: 97TH8237.

IEEE:1997:PAC

[IEE97l] IEEE Computer Society. Technical Committee on Computer Communications, editor. *Proceedings, 22nd annual Conference on Local Computer Networks: LCN '97: November 2–5, 1997, Minneapolis, Minnesota*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. ISBN 0-8186-8141-1, 0-8186-8142-X (casebound), 0-8186-8143-8 (microfiche). ISSN 0742-1303. LCCN TK5105.5 .C82 1997. IEEE Computer Society Press order number PR08141. IEEE Order Plan number 97TB100179.

IEEE:1998:ASF

[IEE98a] IEEE, editor. *39th Annual Symposium on Foundations of Computer Science: proceedings: November 8–11, 1998, Palo Alto, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. CODEN ASFPDV. ISBN 0-8186-9172-7 (softbound), 0-7803-5229-7 (casebound), 0-8186-9174-3 (microfiche). ISSN 0272-5428. LCCN QA267 .S95 1998 Sci-Eng. IEEE Catalog Number 98CB36280. IEEE Computer Society Press order number PR9172.

IEEE:1998:HCC

[IEE98b] IEEE, editor. *Hot chips 10: conference record: August 16–18, 1998, Memorial Auditorium, Stanford University, Palo Alto, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN ???? LCCN ????

IEEE:1998:IIC

[IEE98c] IEEE, editor. *IEEE International Conference on*

Consumer Electronics, Los Angeles, CA, USA, June 2–4, 1998. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. CODEN DTPEEL. ISBN ???? ISSN 0747-668X. LCCN ???? IEEE catalog number 98CH36160.

IEEE:1998:IIF

[IEE98d] IEEE, editor. *IEEE International Forum on Research and Technology Advances in Digital Libraries: ADL'98: proceedings: April 22–24, 1998, Santa Barbara, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN 0-8186-8464-X, 0-8186-8466-6 (microfiche). LCCN TK5103.5.F678 1998. IEEE Computer Society Press Order Number PR08464. IEEE Order Plan Catalog Number 98TB100235.

IEEE:1998:PIC

[IEE98e] IEEE, editor. *Proceedings of the IEEE Conference on Protocols for Multimedia Systems and Multimedia Networking, PROMS-MmNet, Austin, TX, USA, June 28–July 1, 1998*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN 0-8186-8557-3, 0-8186-8559-X (microfiche). LCCN QA76.575.I623 1998. IEEE catalog number 98TB100241. IEEE Computer Society Order Number PR08557.

IEEE:1998:LPA

[IEE98f] IEEE Computer Society. Technical Committee on Computer Communications, editor. *LCN'98: proceedings: 23rd Annual Conference on Local Computer Networks: October 11–14, 1998, Lowell, Massachusetts*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN 0-8186-8810-6, 0-8186-8818-1 (microfiche). LCCN TK5105.5 .C66 1998. IEEE Computer Society Press Order Number PR08810. IEEE Order Plan Catalog Number 98TB100260.

IEEE:1999:ASF

[IEE99a] IEEE, editor. *40th Annual Symposium on Foundations of Computer Science: October 17–19, 1999, New York City, New York*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1999. CODEN ASFPDV. ISBN 0-7695-0409-4 (softbound), 0-7803-5955-0 (casebound), 0-7695-0411-6 (microfiche). ISSN 0272-

5428. LCCN TK7885.A1 S92 1999. IEEE Catalog Number 99CB37039.

IEEE:1999:SWH

[IEE99b] IEEE, editor. *The Seventh Workshop on Hot Topics in Operating Systems: [HotOS-VII]: 29–30 March 1999, Rio Rico, Arizona*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1999. ISBN 0-7695-0237-7, 0-7695-0238-5 (case), 0-7695-0239-3 (microfiche). LCCN QA76.76.O63 W6666 1999. IEEE Computer Society Press order number PR00237.

Itoi:1998:PAM

[IH98] Naomaru Itoi and Peter Honeyman. Pluggable authentication modules for Windows NT. In USENIX [USE98a], page ?? ISBN 1-880446-95-2. LCCN QA76.76.O63 U885 1998. URL http://www.usenix.org/publications/library/proceedings/usenix-nt98/itoi.html; http://www.usenix.org/publications/library/proceedings/usenix-nt98/itoi_slides.

Itoi:1999:PSS

[IH99a] N. Itoi and P. Honeyman. Practical security systems with Smartcards. In IEEE [IEE99b], pages 185–190. ISBN 0-7695-0237-7, 0-7695-0238-5 (case), 0-7695-0239-3 (microfiche). LCCN QA76.76.O63 W6666 1999. IEEE Computer Society Press order number PR00237.

Itoi:1999:SIK

[IH99b] Naomaru Itoi and Peter Honeyman. Smartcard integration with Kerberos V5. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL http://www.usenix.org/publications/library/proceedings/smartcard99/itoiKerberos.html.

Itoi:1999:SUF

[IHR99] Naomaru Itoi, Peter Honeyman, and Jim Rees. SCFS: a UNIX filesystem for Smartcards. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL http://www.usenix.org/publications/library/proceedings/smartcard99/itoiSCFS.html.

IAB:1996:RII

[II96] IAB and IESG. RFC 1984: IAB and IESG statement on cryptographic technology and the Internet, August 1996. URL ftp://ftp.internic.net/rfc/rfc1984.txt; https://www.math.utah.edu/pub/rfc/rfc1984.txt. Status: INFORMATIONAL.

Igarashi:1999:ITP

[IKM99] H. Igarashi, S. Kosue, and M. Miyahara. Individual tactical play and pass with communication between players-team descriptions of Team Miya2. *Lecture Notes in Computer Science*, 1604:364–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Izu:1998:PSE

[IKNY98] T. Izu, J. Kogure, M. Noro, and K. Yokoyama. Parameters for secure elliptic curve cryptosystem — improvements on Schoof's algorithm. *Lecture Notes in Computer Science*, 1431: 253–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Israel:1983:AOS

[IL83] J. E. Israel and T. A. Linden. Authentication in office system internetworks. *ACM Transactions on Office Information Systems*, 1 (3):193–210, July 1983. CODEN ATOSDO. ISSN 0734-2047. URL http://www.acm.org:80.

Impagliazzo:1989:OWF

[IL89] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In IEEE [IEE89], pages 230–235. CODEN ASFPDV. ISBN 0-8186-1982-1 (casebound), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1989. IEEE catalog number 89CH2808-4.

Ilie:1994:CAS

[Ili94] Lucian Ilie. On a conjecture about slender context-free languages. *Theoretical Computer Science*, 132 (1–2):427–434, September 26, 1994. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1994&volume=132&issue=1-2&aid=1683.

Imai:1986:AMC

[IM86] Hideki Imai and Tsutomu Matsumoto. Algebraic methods for constructing asymmetric cryptosystems. *Lecture Notes in Computer Science*, 229:108–119, 1986. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Iwamura:1993:HIM

[IMI93a] K. Iwamura, T. Matsumoto, and H. Imai. High-speed implementation methods for RSA scheme. *Lecture Notes in Computer Science*, 658:221–??, 1993. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Iwamura:1993:HSI

[IMI93b] Keiichi Iwamura, Tsutomu Matsumoto, and Hideki Imai. High-speed implementation methods for RSA scheme. *Lecture Notes in Computer Science*, 658: 221–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580221.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580221.pdf`.

Impagliazzo:1992:PGP

[Imp92] Russell Graham Impagliazzo. *Pseudo-random generators for probabilistic algorithms and for cryptography*. Thesis (Ph.D. in mathematics), Department of Mathematics, University of California, Berkeley, Berkeley, CA, USA, December 1992. 105 pp.

Impagliazzo:1989:ECS

[IN89] Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. In IEEE [IEE89], pages 236–241. CODEN ASFPDV. ISBN 0-8186-1982-1. ISSN 0272-5428. LCCN QA 76 S979 1989. IEEE catalog number 89CH2808-4.

Ito:1999:DPS

[INDI99] N. Ito, K. Nakagawa, X. Du, and N. Ishii. A description-processing system for soccer agents. *Lecture Notes in Computer Science*, 1604: 221–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ingemarsson:1998:E

[Ing98] I. Ingemarsson. Eurocrypt '86. *Lecture Notes in Computer Science*, 1440:55–60, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Instenes:1995:MAA

[Ins95] Shawn Instenes. Musings about authentication. *;login: the USENIX Association newsletter*, 20(4):22–23, August 1995. CODEN LOGNEM. ISSN 1044-6397.

IRD:1979:DVE

[Int79] International Resource Development, Inc. *Data and voice encryption*. International Resource Development, New Canaan, CT, USA, 1979. iv + 124 pp.

IDC:1981:DE

[Int81a] International Data Corporation. Data encryption. Research memorandum IDC #ISPS-M81-10., International Data Corporation, Framingham, MA, USA, October 1981. 30 pp.

IRD:1981:DTV

[Int81b] International Resource Development, Inc. Data, text, and voice encryption equipment. Report 183, IRD, 30 High St., Norwalk, CT 06851, USA, 1981. vi + 154 pp.

IRD:1984:DTV

[Int84] International Resource Development, Inc. Data, text, and voice encryption equipment. Report 630, International Resource Development, 6 Prowitt St., Norwalk, CT 06855, USA, 1984. vi + 184 pp.

IRD:1987:DTV

[Int87] International Resource Development, Inc. Data, text and voice encryption worldwide markets. Report 727, International Resource Development, 6 Prowitt St., Norwalk, CT 06855, USA, February 1987. vii + 197 pp.

IRD:1988:DTV

[Int88] International Resource Development, Inc. Data, text and voice encryption worldwide markets. Report 754, International Resource Development, New Canaan, Conn., U.S.A. (21 Locust Ave., New Canaan 06840), 1988. viii + 285 pp.

Anonymous:1991:IIS

[Int91a] International Organization for Standardization, Geneva, Switzerland. *ISO/IEC. International Standard 9796: Information Technology, Security Techniques: Digital Signature Scheme Giving Message Recovery*, 1991. ?? pp.

IRD:1991:DFV

[Int91b] International Resource Development, Inc. Data, fax and voice encryption equipment, worldwide. Report 782, International Resource Development, New Canaan, CT, USA, December 1991. vi + 298 pp.

Itoh:1994:LDS

[IOS94] Toshiya Itoh, Yuji Ohta, and Hiroki Shizuya. Language dependent secure bit commitment. In Desmedt [Des94b], pages 188–201. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390188.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0839/08390188.pdf`.

Impagliazzo:1989:LPC

[IR89] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In ACM-TOC'89 [ACM89c], pages 44–61. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989.

Ing:1999:SRT

[IR99] S. Ing and S. Rudkin. Simplifying real-time multimedia application development using session descriptions. *Lecture Notes in Computer Science*, 1597: 305–314, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Imai:1993:ACA

[IRM93] Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors. *Advances in cryptology, ASIACRYPT '91: International Conference on the Theory and Application of Cryptology, Fujiyoshida, Japan, November 11–14, 1991: proceedings*, volume 739 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. CODEN LNCSD9. ISBN 0-387-57332-1 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 1991. DM96.00. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0739.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=739.

Irwin:1998:RWD

[Irw98] Lawrence W. Irwin. *The robustness of watermarking in digital images*. Thesis (Ph. D.), University of New Mexico, Albuquerque, NM (??), May 1998. xi + 149 pp.

Ingemarsson:1991:PSS

[IS91] Ingemar Ingemarsson and Gustavus J. Simmons. A protocol to set up shared secret schemes without the assistance of mutually trusted party. *Lecture Notes in Computer Science*, 473: 266–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730266.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730266.pdf.

Ikram:1997:CSE

[IS97] N. Ikram and S. J. Shepherd. A cryptographically secure EW database with selective random access. In ????, editor, *Proceedings of*

IEEE MILCOM '97, Section 37-03, 2–5 November 1997, Monterey, California, page ?? ????, ????, 1997. ISBN ???? LCCN ????

Ikram:1999:UIN

[IS99] N. Ikram and S. J. Shepherd. User identification over network through ID based cryptographic scheme over elliptic curves. *Journal of Computers and Security*, ??(??):??, ???? 1999. Submitted.

Ito:1987:SSS

[ISN87] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structures. In IEEE [IEE87b], pages 99–102. Three volumes. IEEE catalog no. 87CH2520-5.

ISO:1997:ITS

[ISO97] ISO/IEC 10118. *Information technology — Security techniques — Hash-functions, Part 1: General (IS, 1994); Part 2: Hash-functions using an n-bit block cipher algorithm, (IS, 1994); Part 3: Dedicated hash-functions (IS, 1997); Part 4: Hash-functions using modular arithmetic, (FCD, 1997)*. International Organization for Standardization, Geneva, Switzerland, 1997. ?? pp.

Isselhorst:1990:UFP

[Iss90] Hartmut Isselhorst. The use of fractions in public-key cryptosystems. *Lecture Notes in Computer Science*, 434:47–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340047.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340047.pdf`.

Itoh:1991:CFI

[Ito91] Toshiya Itoh. Characterization for a family of infinitely many irreducible equally spaced polynomials. *Information Processing Letters*, 37(5):273–277, March 14, 1991. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Iversen:1991:CSC

[Ive91] Kenneth R. Iversen. A cryptographic scheme for computerized general elections. *Lecture Notes in Computer Science*, 576: 405–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760405.htm;`

http://link.springer-ny.com/link/service/series/0558/papers/0576/05760405.pdf.

Ingemarsson:1981:UAS

[IW81] Ingemar Ingemarsson and C. K. Wong. Use authentication scheme for shared data based on a trap-door one-way function. *Information Processing Letters*, 12(2):63–67, April 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Imai:1998:PKC

[IZ98] Hideki Imai and Yuliang Zheng, editors. *Public key cryptography: first International Workshop on Practice and Theory in Public Key Cryptography, PKC '98, Pacifico Yokohama, Japan, February 5–6, 1998: proceedings*, volume 1431 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-64693-0 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I567 1998 Bar.

Imai:1999:PKC

[IZ99] Hideki Imai and Yuliang Zheng, editors. *Public key cryptography: second International Workshop on Practice and Theory in Public Key Cryptography, PKC'99, Kamakura, Japan, March 1–3, 1999: proceedings*, volume 1560 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-65644-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1560.

Jaburek:1990:GGP

[Jab90] W. J. Jaburek. A generalization of El Gamal's public key cryptosystem. *Lecture Notes in Computer Science*, 434:23–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340023.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340023.pdf.

Jackson:1987:NTS

[Jac87] T. H. Jackson. *From number theory to secret codes*. Hilger, Bristol, UK, 1987. ISBN 0-85274-077-8 (paperback), 0-85274-078-6. vi + 86 pp. LCCN Z104 .J3 1987.

Jackson:1990:SITa

[Jac90a] Keith M. Jackson. *Secure information transfer:*

PC encryption: a practical guide. Blackwell Scientific Publications, Oxford, UK; Boston, MA, USA, 1990. ISBN 0-632-02664-2. ix + 182 pp. LCCN QA76.9.A25J32 1990.

Jackson:1990:SITb

[Jac90b] Keith M. Jackson. *Secure information transfer: PC encryption: a practical guide*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1990. ISBN 0-8493-7711-0. ix + 182 pp. LCCN QA 76.9 A25 J32 1990.

Jackson:1996:AAC

[Jac96] I. W. Jackson. Anonymous addresses and confidentiality of location. In Anderson [And96c], pages 115–120. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054431.html`.

Jakobsson:1995:BUU

[Jak95] M. Jakobsson. Blackmailing using undeniable signatures. *Lecture Notes in Computer Science*, 950: 425–427, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jakobsen:1998:CBC

[Jak98] Thomas Jakobsen. Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree. *Lecture Notes in Computer Science*, 1462: 212–222, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jakobsen:1999:HOC

[Jak99a] Thomas Jakobsen. *Higher-order cryptanalysis of block ciphers*. Ph.D. thesis, Department of Mathematics, Technical University of Denmark, Lyngby, Denmark, 1999. viii + 110 pp.

Jakobsson:1999:MCM

[Jak99b] M. Jakobsson. Mini-cash: a minimalistic approach to E-commerce. *Lecture Notes in Computer Science*, 1560: 122–135, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jakobsson:1999:QCA

[Jak99c] Markus Jakobsson. On quorum controlled asymmetric proxy re-encryption. *Lecture Notes in Computer Science*, 1560:112–121, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/`

link/service/series/0558/bibs/1560/15600112.htm; http://link.springer-ny.com/link/service/series/0558/papers/1560/15600112.pdf.

Jamieson:1998:UEP

[Jam98] Lauren Jamieson. Unveiling the extraordinary possibilities and implicit threats of online communication. *Asterisk: the journal of computer documentation*, 22(4): 27–31, November 1998. CODEN ASTRF7. ISSN 0731-1001.

Jantke:1995:RSI

[Jan95] K. P. Jantke. Reflecting and self-confident inductive inference machines. *Lecture Notes in Computer Science*, 997:282–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Janecek:1999:AVR

[Jan99] P. Janecek. Applying visualization research towards design. *Lecture Notes in Computer Science*, 1614: 817–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jarecki:1996:PSS

[Jar96] S. Jarecki. Proactive secret sharing and public key cryptosystems. Masters thesis, MIT, Cambridge, MA, USA, 1996.

Jarvis:1997:GB

[Jar97] Peter Jarvis. The German battleships. Technical report, Bletchley Park Trust, Bletchley Park, UK, 1997. ???? pp.

Jaspan:1996:DWE

[Jas96] Barry Jaspan. Dual-workfactor encrypted key exchange: Efficiently preventing password chaining and dictionary attacks. In USENIX [USE96e], pages 43–50. ISBN 1-880446-79-0. LCCN QA76.9.A25 U83 1996. URL http://www.usenix.org/publications/library/proceedings/sec96/jaspan.html.

Jaeger:1993:LCC

[JC93] J. L. Jaeger and R. T. Carlson. Laser communications for covert links. In Anonymous [Ano93h], pages 95–106. ISBN ???? LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/024130.html.

Jan:1998:PWP

[JC98] Jinn-Ke Jan and Yu-Yii Chen. "paramita wisdom" password authentication scheme without verification tables. *The Journal of Systems and Software*, 42(1):45–57, July 1, 1998. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.elsevier.com/cas/tree/store/jss/sub/1998/42/1/6026.pdf.

Johnson:1991:TSS

[JD91] D. B. Johnson and G. M. Dolan. Transaction Security System extensions to the Common Cryptographic Architecture. *IBM Systems Journal*, 30(2): 230–243, 1991. CODEN IBMSA7. ISSN 0018-8670.

Johnson:1991:CCA

[JDK+91] D. B. Johnson, G. M. Dolan, M. J. Kelly, A. V. Le, and S. M. Matyas. Common Cryptographic Architecture Cryptographic Application Programming Interface. *IBM Systems Journal*, 30(2):130–150, 1991. CODEN IBMSA7. ISSN 0018-8670.

Jeffery:1986:GCC

[Jef86] Keith Jeffery. The Government Code and Cypher School; A memorandum by Lord Curzon. *Intelligence and National Security*, 1 (3):454–??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Jensen:1999:GDT

[Jen99] F. V. Jensen. Gradient descent training of Bayesian networks. *Lecture Notes in Computer Science*, 1638: 190–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jenkins:19xx:IFC

[Jenxx] Bob Jenkins, Jr. ISAAC: a fast cryptographic random number generator. Web site, 19xx. URL http://burtleburtle.net/bob/rand/isaacafa.html. ISAAC (Indirection, Shift, Accumulate, Add, and Count) is based on cryptographic principles, and generates 32-bit random numbers. ISAAC-64 is similar, but requires 64-bit arithmetic, and generates 64-bit results.

Jevons:1874:PS

[Jev74] W. Stanley Jevons. *The Principles of Science*. ????, ????, 1874. ??–?? pp.

Joyce:1990:IAB

[JG90] Rick Joyce and Gopal Gupta. Identity authentication based on keystroke latencies. *Communications of the Association for Computing Machinery*, 33(2):168–176, February 1990. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/75582.html.

Joux:1995:PAA

[JG95] A. Joux and L. Granboulan. A practical attack against knapsack based hash functions. *Lecture Notes in Computer Science*, 950: 58–66, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jian:1999:SDM

[Jia99] Z. Jian. System description: MCS: Model-based conjecture searching. *Lecture Notes in Computer Science*, 1632:393–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jolitz:1991:PUI

[JJ91] William Frederick Jolitz and Lynne Greer Jolitz. Porting UNIX to the 386. the initial root filesystem. *Dr. Dobb's Journal of Software Tools*, 16(5):46, 48, 50, 52–54, May 1991. CODEN DDJOEB. ISSN 1044-789X.

Jolitz:1995:RNS

[JJ95] William F. Jolitz and Lynne Greer Jolitz. Role-based network security. *Dr. Dobb's Journal of Software Tools*, 20(5):80, 82, 84–85, May 1995. CODEN DDJOEB. ISSN 1044-789X.

Johnson:1998:ESS

[JJ98a] N. F. Johnson and S. Jajodia. Exploring steganography: Seeing the unseen. *Computer*, 31(2):26–34, February 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1048.html`.

Johnson:1998:CPE

[JJ98b] Neil F. Johnson and Sushil Jajodia. Computing practices: Exploring steganography: Seeing the unseen. *Computer*, 31(2):26–34, February 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://pdf.computer.org/co/books/co1998/pdf/r2026.pdf`; `http://www.computer.org/computer/co1998/r2026abs.htm`.

Johnson:1998:SIC

[JJ98c] Neil F. Johnson and Sushil Jajodia. Steganalysis of images created using current steganography software. *Lecture Notes in Computer Science*, 1525: 273–289, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250273.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1525/15250273.pdf`.

Johansson:1999:FCA

[JJ99a] T. Johansson and F. Joensson. Fast correlation attacks based on turbo code techniques. In Wiener [Wie99], pages 181–197. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Johansson:1999:IFC

[JJ99b] T. Johansson and F. Joensson. Improved fast correlation attacks on stream ciphers via convolutional codes. *Lecture Notes in Computer Science*, 1592: 347–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jakobsen:1997:IAB

[JK97] T. Jakobsen and L. R. Knudsen. The interpolation attack on block ciphers. *Lecture Notes in Computer Science*, 1267:28–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jun:1999:IRN

[JK99] Benjamin Jun and Paul Kocher. The Intel random number generator. White paper prepared for Intel Corporation, Cryptography Research, Inc., Menlo Park, CA, USA, April 22, 1999. URL `http://www.cryptography.com/intelRNG.pdf`.

Jonker:1999:VTK

[JKVP99] C. M. Jonker, R. Kremer, P. Van Leeuwen, and D. Pan. Visual and textual knowledge representation in DESIRE. *Lecture Notes in Computer Science*, 1611:306–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jones:1975:ESP

[JL75] Anita K. Jones and Richard J. Lipton. The enforcement of security policies for computation. *Operating Systems Review*, 9(5): 197–206, November 1975. CODEN OSRED8. ISSN 0163-5980.

Johnson:1994:HKD

[JLM+94] D. Johnson, A. Le, W. Martin, S. Matyas, and J. Wilkins. Hybrid key distribution scheme giving key record recovery. *IBM Technical Disclosure Bulletin*, 37(2A):5–16, February 1994. CODEN IBMTAA. ISSN 0018-8689.

Juels:1997:SBD

[JLO97] Ari Juels, Michael Luby, and Rafail Ostrovsky. Security of blind digital signatures. *Lecture Notes in Computer Science*, 1294: 150–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/`

link/service/series/0558/bibs/1294/12940150.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940150.pdf.

Jurgensen:1984:SRI

[JM84] H. Jürgensen and D. E. Matthews. Some results on the information theoretic analysis of cryptosystems. In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 303–356. Plenum, New York, 1984.

Jackson:1993:CAG

[JM93] W.-A. Jackson and K. M. Martin. Cumulative arrays and geometric secret sharing schemes. *Lecture Notes in Computer Science*, 718:48–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Janwa:1996:MPK

[JM96a] Heeralal Janwa and Oscar Moreno. McEliece public key cryptosystems using algebraic-geometric codes. *Designs, Codes, and Cryptography*, 8(3): 293–307, 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Johnson:1996:AEE

[JM96b] Don B. Johnson and Stephen M. Matyas. Asymmetric encryption: Evolution and enhancements. *CryptoBytes*, 2(1):1, 3–6, Spring 1996. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto2n1.pdf.

Jurisic:1997:ECC

[JM97] Aleksandar Jurisic and Alfred J. Menezes. Elliptic curves and cryptography. *Dr. Dobb's Journal of Software Tools*, 22(4):26–??, April 1997. CODEN DDJOEB. ISSN 1044-789X.

Jakobsson:1999:IMI

[JM99] M. Jakobsson and J. Mueller. Improved magic ink signatures using hints. In Franklin [Fra99], pages 253–267. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Johnson:1994:CDM

[JMLW94] D. B. Johnson, S. M. Matyas, A. V. Le, and J. D. Wilkins. The Commercial Data Masking Facility (CDMF) data privacy algorithm. *IBM Journal of Research and Development*, 38(2):217–226, March 1994. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL http://www.almaden.ibm.com/journal/rd38-2.html#eight.

Jackson:1994:MTS

[JMO94] W. Jackson, K. Martin, and C. O'Keefe. Multisecret threshold schemes. In Stinson [Sti94], pages 126–135. CODEN LNCSD9. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1993. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0773.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=773.

Jackson:1995:ESS

[JMO95a] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe. Efficient secret sharing without a mutually trusted authority. *Lecture Notes in Computer Science*, 921:183–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jackson:1995:SMS

[JMO95b] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe. On sharing many secrets. *Lecture Notes in Computer Science*, 917:42–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jerichow:1998:RTM

[JMP+98] A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitzmann, and M. Waidner. Real-time mixes: a bandwidth-efficient anonymity protocol. *IEEE Journal on Selected Areas in Communications*, 16(4): 495–509, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072127.html.

Jakobsson:1996:DVP

[JMSI96] Jakobsson, Markus, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In Maurer [Mau96b], pages 143–154. CODEN LNCSD9. ISBN 3-540-61186-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1996. URL http://www.bell-labs.com/user/markusj/dvp.ps. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Jarecki:1997:EMS

[JO97] S. Jarecki and A. Odlyzko. An efficient micropayment system based on probabilistic polling. *Lecture Notes in Computer Science*, 1318:173–191, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.research.att.com/~amo/doc/polling.pdf; http://www.research.att.com/~amo/doc/polling.ps; http://www.research.att.com/~amo/doc/polling.tex.

Joesang:1998:SMA

[Joe98] A. Joesang. A subjective metric of authentication. *Lecture Notes in Computer Science*, 1485:329–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Johnson:1989:BDC

[Joh89] Michael Paul Johnson. Beyond DES: data compression and the MPJ encryption algorithm. Thesis (M.S.), University of Colorado at Colorado Springs, Colorado Springs, CO, USA, 1989. viii + 127 pp.

Johnson:1990:EDE

[Joh90] Craig W. Johnson. An examination of the Data Encryption Standard and its use in the commercial environment. Thesis (M.S.), University of Colorado, Boulder, CO, USA, 1990. xi + 207 pp.

Johansson:1994:CPA

[Joh94] Thomas Johansson. On the construction of perfect authentication codes that permit arbitration. *Lecture Notes in Computer Science*, 773:343–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730343.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730343.pdf.

Johnson:1995:ACD

[Joh95] Thomas R. Johnson. *American cryptology during the Cold War, 1945–1989*. Series VI the NSA period 1952 - present. Center for Cryptologic History, National Security Agency, Fort George G. Meade, MD, USA, 1995. ???? pp. LCCN JZ5630 .J64 1995 Electronic. URL http://worldcat.org/oclc/275579995/viewonline; http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/index.htm; http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-1.pdf; http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/NSA-2.pdf; http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-3.pdf; http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-4.pdf; http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-5.pdf; http://www.gwu.edu/~nsarchiv/

NSAEBB/NSAEBB260/nsa-6.pdf.

Johnson:1996:LP

[Joh96] Michael K. Johnson. Lurking with PGP. *Linux Journal*, 32:??, December 1996. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Johnson:1997:SP

[Joh97a] A. Johnson. Steganography for DOS programmers. *Dr. Dobb's Journal of Software Tools*, ??(261):48–51, January 1997. CODEN DDJOEB. ISSN 1044-789X. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054140.html.

Johnson:1997:SPS

[Joh97b] Alan Johnson. Steganography for DOS programmers — steganography is a branch of cryptography that deals with concealing messages. *Dr. Dobb's Journal of Software Tools*, 22(1):48–??, January 1997. CODEN DDJOEB. ISSN 1044-789X.

JohnByrne:1998:CEC

[Joh98] Cipher A. Deavours John Byrne, Louis Kruh. Chaocipher enters the computer age when its method is disclosed to Cryptologia's editors. In Deavours et al. [DKK+98], pages 317–322. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Johnson:1999:LES

[Joh99] Don Johnson. Letter to the editor: a short history of Triple DES and ANSI X9.F.1. *CryptoBytes*, 4 (2):2, Winter 1999. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n2.pdf.

Jolitz:1995:PB

[Jol95] Lynne Greer Jolitz. Programmer's bookshelf. *Dr. Dobb's Journal of Software Tools*, 20(8):133–??, August 1995. CODEN DDJOEB. ISSN 1044-789X.

Jones:1978:WWB

[Jon78a] R. V. (Reginald Victor) Jones. *The Wizard War: British Scientific Intelligence, 1939–1945*. Coward, McCann and Geoghegan, New York, NY, USA, 1978. ISBN 0-698-10896-5. xx + 556 + 16 pp. LCCN D810.C88 J66 1978. URL https://en.wikipedia.org/wiki/Reginald_Victor_Jones.

Jones:1978:MSW

[Jon78b] Reginald V. Jones. *Most secret war: [British scientific intelligence, 1939–1945]*. Hamilton, London, UK, 1978. ISBN 0-241-89746-7. xx + 556 + 16 pp. LCCN ????

Jones:1986:DEB

[Jon86] John W. Jones. Data encryption based on the logarithm problem. Thesis (M.A.Sc.), University of Ottawa, Ottawa, ON, Canada, 1986. 2 microfiches (103 fr.).

Jones:1990:PKC

[Jon90] M. Christopher W. Jones. A public key cryptosystem as hard as factorisation. *Irish Math. Soc. Bull.*, 24:59–66, 1990. ISSN 0791-5578.

Josse:1885:CSA

[Jos85] H. (Henri) Jossé. *La cryptographie et ses applications à l'art militaire*. Libraire militaire de L. Baudoin, Paris, France, 1885. 103 pp. LCCN Z104 .J67 1885.

JCryptology:1988:JCJ

[Jou88] *Journal of cryptology: the journal of the International Association for Cryptologic Research*, page various, 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/index.htm`. Springer International, New York, NY, USA. Appears three times a year.

Juels:1996:HCC

[JP96] Ari Juels and Marcus Peinado. Hidden cliques as cryptographic keys. Report UCB/CSD 96/912, University of California, Berkeley, Computer Science Division, Berkeley, CA, USA, September 11, 1996. 8 pp.

Jaeger:1999:FCD

[JPLI99] Trent Jaeger, Atul Prakash, Jochen Liedtke, and Nayeem Islam. Flexible control of downloaded executable content. *ACM Transactions on Information and System Security*, 2(2):177–228, May 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-2/p177-jaeger/`.

Joye:1997:PFR

[JQ97] Marc Joye and Jean-Jacques Quisquater. Protocol failures for RSA-like functions using Lucas sequences and elliptic curves. *Lecture Notes in Computer Science*, 1189:93–100, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Joye:1998:CRT

[JQ98a] Marc Joye and Jean-Jacques Quisquater. Cryptanalysis of RSA-type cryptosystems: a visit. In

Wright and Neumann [WN98b], pages 21–31. ISBN 0-8218-0832-X. LCCN TK5105.5 .N4668 1998.

Joye:1998:REC

[JQ98b] Marc Joye and Jean-Jacques Quisquater. Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams. *Designs, Codes, and Cryptography*, 14(1):53–56, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Joye:1997:RTS

[JQBD97] M. Joye, J. J. Quisquater, F. Bao, and R. H. Deng. RSA-type signatures in the presence of transient faults. *Lecture Notes in Computer Science*, 1355:155–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jurgensen:1996:TFC

[JR96] H. Jürgensen and L. Robbins. Towards foundations of cryptography: Investigation of perfect secrecy. *J.UCS: Journal of Universal Computer Science*, 2(5):347–379, May 28, 1996. ISSN 0948-6968. URL `http://www.iicm.edu/jucs_2_5/towards_foundations_of_cryptography`.

Jones:1993:DAC

[JS93a] G. Jones and M. Sheeran. Designing arithmetic circuits by refinement in Ruby. *Lecture Notes in Computer Science*, 669:107–136, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Joux:1993:CAK

[JS93b] Antoine Joux and Jacques Stern. Cryptanalysis of another knapsack cryptosystem. *Lecture Notes in Computer Science*, 739:470–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Johansson:1995:AIA

[JS95a] T. Johansson and B. Smeets. On A02-codes including arbiter's attacks. *Lecture Notes in Computer Science*, 950:456–460, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Johansson:1995:CIA

[JS95b] Thomas Johansson and Bernard J. M. Smeets. On A^2-codes including arbiter's attacks. *Lecture Notes in Computer Science*, 950: 456–460, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500456.htm;`

http://link.springer-ny.com/link/service/series/0558/papers/0950/09500456.pdf.

Jakobsson:1999:SAE

[JSY99] Markus Jakobsson, Julien P. Stern, and Moti Yung. Scramble all, encrypt small. In Knudsen [Knu99c], pages 95–111. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1636/16360095.htm; http://link.springer-ny.com/link/service/series/0558/papers/1636/16360095.pdf.

Jiwa:1994:BBA

[JSZ94] A. Jiwa, J. Seberry, and Y. Zheng. Beacon based authentication. *Lecture Notes in Computer Science*, 875: 125–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jan:1996:SIE

[JT96] Jinn-Ke Jan and Yuh-Min Tseng. On the security of image encryption method. *Information Processing Letters*, 60(5):261–265, December 8, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Jan:1997:SEV

[JT97a] Jinn-Ke Jan and Chih-Chang Tai. A secure electronic voting protocol with IC cards. *The Journal of Systems and Software*, 39 (2):93–101, November 1997. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Jan:1997:SIE

[JT97b] Jinn-Ke Jan and Yuh-Min Tseng. On the security of image encryption method. *Information Processing Letters*, 60(5):261–265, January 21, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Juenemann:1981:DES

[Jue81] Robert R. Juenemann. The Data Encryption Standard vs. exhaustive search. Report, Satellite Business Systems, McLean, VA, USA, February 5, 1981.

Juels:1999:TTS

[Jue99] A. Juels. Trustee tokens: Simple and practical anonymous digital coin tracing. In Franklin [Fra99], pages 29–45. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Jung:1987:IRC

[Jun87] Achim Jung. Implementing the RSA cryptosystem.

Computers and Security, 6 (4):342–350, August 1987. CODEN CPSEDU. ISSN 0167-4048.

Jung:1988:IRC

[Jun88] A. Jung. Implementing the RSA cryptosystem. *Computers and Security*, 7(5):510–511, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902131`.

Jungnickel:1996:DFG

[Jun96] D. Jungnickel. *Designs and finite geometries*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1996. ISBN 0-7923-9730-4. 254 pp. LCCN QA166.25 .D46 1996. Reprint of a special issue of Designs, codes, and cryptography, an international journal, volume 8, no. 1/2 (1996).

Jung:1999:EMA

[Jun99] C. Jung. Emergent mental attitudes in layered agents. *Lecture Notes in Computer Science*, 1555:195–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jurgen:1986:SEI

[Jur86] R. K. Jurgen. The specialties: Experts identify the most outstanding developments or the most difficult problems in their fields. *IEEE Spectrum*, 23(1):86–87, January 1986. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Jutla:1998:GBA

[Jut98] C. S. Jutla. Generalized birthday attacks on unbalanced Feistel networks. *Lecture Notes in Computer Science*, 1462:186–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Just:1996:AMP

[JV96] M. Just and S. Vaudenay. Authenticated multi-party key agreement. *Lecture Notes in Computer Science*, 1163:36–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jakubowski:1998:CSP

[JV98a] M. H. Jakubowski and R. Venkatesan. The chain and sum primitive and its applications to MACs and stream ciphers. *Lecture Notes in Computer Science*, 1403:281–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jeannerod:1998:GEE

[JV98b] C. P. Jeannerod and J. Visconti. Global error estimation for index-1 and -2 DAEs. *Numerical Algorithms*, 19(1–4):111–125, September 1998. CODEN NUALEG. ISSN 1017-1398 (print), 1572-9265 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/5058/16/11/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/5058/16/11/fulltext.pdf. Differential algebraic equations (Grenoble, 1997).

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].

Jakobsson:1996:OAB

[JY96] M. Jakobsson and M. Yung. On oblivious, agnostic, and blindfolded provers. In Koblitz [Kob96], pages 186–200. CODEN LNCSD9. ISBN 3-540-61512-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1996. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1109.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1109. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Joye:1998:IBS

[JY98] Marc Joye and Sung-Ming Yen. ID-based secret-key cryptography. *Operating Systems Review*, 32(4):33–39, October 1998. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kompella:1991:FCC

[KA91] K. Kompella and L. Adleman. Fast checkers for cryptography. *Lecture Notes in Computer Science*, 537:515–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kent:1998:RIA

[KA98a] S. Kent and R. Atkinson. RFC 2402: IP authentication header, November 1998. URL ftp://ftp.internic.net/rfc/rfc1826.txt; ftp://ftp.internic.net/rfc/rfc2402.txt; https:/

/www.math.utah.edu/pub/rfc/rfc1826.txt; https://www.math.utah.edu/pub/rfc/rfc2402.txt. Obsoletes RFC1826 [Atk95a]. Status: PROPOSED STANDARD.

Kent:1998:RIE

[KA98b] S. Kent and R. Atkinson. RFC 2406: IP Encapsulating Security Payload (ESP), November 1998. URL ftp://ftp.internic.net/rfc/rfc1827.txt; ftp://ftp.internic.net/rfc/rfc2406.txt; https://www.math.utah.edu/pub/rfc/rfc1827.txt; https://www.math.utah.edu/pub/rfc/rfc2406.txt. Obsoletes RFC1827 [Atk95b]. Status: PROPOSED STANDARD.

Koutsoukos:1999:HCS

[KA99] X. D. Koutsoukos and P. J. Antsaklis. Hybrid control systems using timed Petri nets: Supervisory control design based on invariant properties. *Lecture Notes in Computer Science*, 1567: 142–162, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kahn:1963:PNU

[Kah63] David Kahn. *Plaintext in the new unabridged: an examination of the definitions on cryptology in Webster's Third New International Dictionary*. Crypto Press, New York, NY, USA, 1963. 35 pp.

Kahn:1966:MC

[Kah66] David Kahn. Modern cryptology. *Scientific American*, 215(1):38–46, July 1966. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v215/n1/pdf/scientificamerican0766-38.pdf.

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 0-02-560460-0, 0-297-76785-2. xvi + 576 pp. LCCN Z103 .K28 1974.

Kahn:1976:TC

[Kah76] David Kahn. Tapping computers. *New York Times*, ??(??):??, April 3, 1976. CODEN NYTIAO. ISSN 0362-4331 (print), 1542-667X, 1553-8095.

Kahn:1979:CGP

[Kah79] David Kahn. Cryptology goes public. *Foreign affairs (Council on Foreign Relations)*, 58(1):141–159, Fall 1979.

Kahn:1982:GLC

[Kah82] David Kahn. The grand lines of cryptology's development. *Computers and Security*, 1(3):245–248, November 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404882900426.

Kahn:1983:KCS

[Kah83] David Kahn. *Kahn on codes: secrets of the new cryptology*. MacMillan Publishing Company, New York, NY, USA, 1983. ISBN 0-02-560640-9. viii + 343 pp. LCCN Z103 .K29 1983.

Kahn:1984:COS

[Kah84] D. Kahn. Cryptology and the origins of spread spectrum. *IEEE Spectrum*, 21(9):70–80, September 1984. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1009.html.

Kahn:1991:SER

[Kah91a] David Kahn. *Seizing the Enigma: the race to break the German U-boat codes, 1939–1943*. Houghton-Mifflin, Boston, MA, USA, 1991. ISBN 0-395-42739-8. xii + 336 pp. LCCN D810.C88 K34 1991.

Kahn:1991:WWW

[Kah91b] David Kahn. Why weren't we warned? *MHQ: Quarterly Journal of Military History*, 4(1):50–59, Autumn 1991. ISSN 1040-5992. URL http://www.historynet.com/why-werent-we-warned.htm.

Kahn:1996:HS

[Kah96a] D. Kahn. The history of steganography. In Anderson [And96c], pages 1–5. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054141.html.

Kahn:1996:CSS

[Kah96b] 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].

Kahn:1998:EC

[Kah98a] David Kahn. An Enigma chronology. In Deavours et al. [DKK+98], pages 423–432. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Kahn:1998:PHI

[Kah98b] David Kahn. Pearl Harbor and the inadequacy of cryptanalysis. In Deavours et al. [DKK+98], pages 35–56. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Kahn:1998:RMU

[Kah98c] David Kahn. Roosevelt, MAGIC, and ULTRA. In Deavours et al. [DKK+98], pages 123–153. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Kak:1983:EMP

[Kak83] Subhash C. Kak. Exponentiation modulo a polynomial for data security. *International Journal of Computer and Information Sciences*, 12(5):337–346, October 1983. CODEN IJCIAH. ISSN 0091-7036.

Kak:1984:MPK

[Kak84] S. C. Kak. On the method of puzzles for key distribution. *International Journal of Computer and Information Sciences*, 13(2):103–109, April 1984. CODEN IJCIAH. ISSN 0091-7036.

Kak:1985:EEC

[Kak85] Subhash C. Kak. Encryption and error-correction coding using D sequences. *IEEE Transactions on Computers*, 34(9):803–809, 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Koc:1996:ACM

[KAK96] Çetin Kaya Koç, Tolga Acar, and Burton S. Kaliski, Jr. Analyzing and comparing Montgomery multiplication algorithms — assessing five algorithms that speed up modular exponentiation, the most popular method of encrypting and signing digital data. *IEEE Micro*, 16

(3):26–33, May/June 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Kaliski:1984:AWA

[Kal84] Burton Stephen Kaliski, Jr. Analysis of Wyner's analog encryption scheme. Thesis (B.S.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1984. 97 pp. Supervised by Ronald L. Rivest.

Kaliski:1985:WAE

[Kal85] Burt S. Kaliski. Wyner's analog encryption scheme: Results of a simulation. In Blakley and Chaum [BC85], pages 83–94. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=83`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Kaliski:1991:MMD

[Kal91] Burt S. Kaliski Jr. The MD4 message digest algorithm. *Lecture Notes in Computer Science*, 473: 492–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730492.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0473/04730492.pdf`.

Kaliski:1992:MAC

[Kal92] Burton S. Kaliski, Jr. Multiple-precision arithmetic in C. *Dr. Dobb's Journal of Software Tools*, 17(8):40, 42, 44, 46–48, 116–119, August 1992. CODEN DDJOEB. ISSN 1044-789X.

Kaliski:1993:SES

[Kal93a] Burt Kaliski. A survey of encryption standards. *IEEE Micro*, 13(6):74–81, November/December 1993. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Kaliski:1993:ZBA

[Kal93b] Burton S. Kaliski, Jr. The Z80180 and big-number arithmetic. *Dr. Dobb's Journal of Software Tools*, 18(9):50, 52, 54, 56, 58, 90–91, September 1993. CO-

DEN DDJOEB. ISSN 1044-789X.

Kaliski:1995:MIA

[Kal95] Burton S. Kaliski, Jr. The Montgomery inverse and its applications. *IEEE Transactions on Computers*, 44(8):1064–1065, August 1995. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=403725.

Kaliski:1997:IPS

[Kal97a] B. S. Kaliski. IEEE P1363: a standard for RSA, Diffie–Hellman and elliptic-curve cryptography [abstract]. *Lecture Notes in Computer Science*, 1189: 117–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kaliski:1997:PNG

[Kal97b] Burt Kaliski. PKCS: The next generation, chapter 2. *CryptoBytes*, 3(2): 15, Autumn 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n2.pdf.

Kaliski:1997:ACC

[Kal97c] Burton S. Kaliski, editor. *Advances in cryptology, CRYPTO '97: 17th annual international cryptology conference, Santa Barbara, California, USA, August 17–21, 1997: proceedings*, volume 1294 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-63384-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1997. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1294.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1294.

Kaliski:1998:C

[Kal98a] B. Kaliski. Crypto '97. *Lecture Notes in Computer Science*, 1440:223–232, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kaliski:1998:RPRa

[Kal98b] B. Kaliski. RFC 2313: PKCS #1: RSA encryption version 1.5, March 1998. URL ftp://ftp.internic.net/rfc/rfc2313.txt; ftp://ftp.internic.net/rfc/rfc2437.txt; https://www.math.utah.edu/pub/rfc/rfc2313.txt; https://www.math.utah.edu/pub/rfc/rfc2437.txt. Obsoleted by RFC2437

[KS98a]. Status: INFORMATIONAL.

Kaliski:1998:RPCb

[Kal98c] B. Kaliski. RFC 2314: PKCS #10: Certification request syntax version 1.5, March 1998. URL ftp://ftp.internic.net/rfc/rfc2314.txt; https://www.math.utah.edu/pub/rfc/rfc2314.txt. Status: INFORMATIONAL.

Kaliski:1998:RPCc

[Kal98d] B. Kaliski. RFC 2315: PKCS #7: Cryptographic message syntax version 1.5, March 1998. URL ftp://ftp.internic.net/rfc/rfc2315.txt; https://www.math.utah.edu/pub/rfc/rfc2315.txt. Status: INFORMATIONAL.

Kaliski:1998:EDF

[Kal98e] B. S. Kaliski. ECC/DLP and factoring-based cryptography: a tale of two families. *Lecture Notes in Computer Science*, 1514:50–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kaliski:1998:RPCa

[Kal98f] B. S. Kaliski. RFC 2315: PKCS #7: Cryptographic message syntax version 1, March 1998. URL ftp://ftp.internic.net/rfc/rfc2315.txt; https://www.math.utah.edu/pub/rfc/rfc2315.txt. Status: INFORMATIONAL.

Kaliski:1998:REC

[Kal98g] Burton S. Kaliski, Jr. Recommendations on elliptic curve cryptosystems. Technical report, RSA Data Security, Inc., Redwood City, CA, USA, March 1998. URL http://www.rsasecurity.com/rsalabs/ecc/ecc_recommendations.html.

Kaliski:1999:ESP

[Kal99] Burton S. Kaliski Jr. Emerging standards for public-key cryptography. *Lecture Notes in Computer Science*, 1561:87–104, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1561/15610087.htm; http://link.springer-ny.com/link/service/series/0558/papers/1561/15610087.pdf.

Kaneshige:1996:ITC

[Kan96] Thomas Kaneshige. Industry trends: Cyberwar; Clipper chip; network computers. *Computer*, 29(7):20–23, July 1996. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). Contains news brief: Lots of Java brewing at conference.

Kaps:1998:HSF

[Kap98] Jens-Peter Kaps. High speed FPGA architectures for the Data Encryption Standard. Thesis (M.S.), Worcester Polytechnic Institute, Worcester, MA, USA, 1998. ix + 114 pp.

Karger:1985:ADA

[Kar85] Paul A. Karger. Authentication and discretionary access control in computer networks. *Computer Networks and ISDN Systems*, 10(1):27–37, August 1985. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic).

Karger:1986:ADA

[Kar86] Paul A. Karger. Authentication and discretionary access control in computer networks. *Computers and Security*, 5(4):314–324, December 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886900520`.

Karger:1987:LDP

[Kar87] P. Karger. Limiting the damage potential of discretionary Trojan horses. In IEEE [IEE87c], pages 32–37. ISBN 0-8186-8771-1 (hardback), 0-8186-0771-8 (paperback), 0-8186-4771-X (microfiche). LCCN QA 76.9 A25 I43 1987. IEEE catalog number 87CH2416-6. Computer Society Order Number 771.

Kari:1989:CBP

[Kar89a] Jarkko Kari. A cryptosystem based on propositional logic. *Lecture Notes in Computer Science*, 381: 210–219, 1989. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kari:1989:OCP

[Kar89b] Jarkko Kari. Observations concerning a public-key cryptosystem based on iterated morphisms. *Theoretical Computer Science*, 66 (1):45–53, August 2, 1989. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Karkare:1996:SEA

[Kar96] Sonia Karkare. Secure email architecture using PGP at the Timken Company. Thesis (M.S.), Department of Mathematical and Computer Science, Kent State University, Kent, OH, USA, 1996. xv + 169 pp.

Kasiski:1863:GDG

[Kas63] Friedrich Wilhelm Kasiski. *Die Geheimschriften und die Dechiffrirkunst, Mit besonderer Berücksichtigung der deutschen und französischen Sprache. (German) [Secret* *writing and the art of deciphering, with special reference to the German and French languages]*. E. S. Mittler und Sohn, Berlin, Germany, 1863. viii + 95 + 4 pp. LCCN ????

Kastenholz:1996:RVP

[Kas96] F. Kastenholz. RFC 1915: Variance for the PPP connection control protocol and the PPP encryption control protocol, February 1996. URL `ftp://ftp.internic.net/rfc/bcp3.txt`; `ftp://ftp.internic.net/rfc/rfc1915.txt`; `https://www.math.utah.edu/pub/rfc/bcp3.txt`; `https://www.math.utah.edu/pub/rfc/rfc1915.txt`. See also BCP0003 [?]. Status: BEST CURRENT PRACTICE.

Kalipha:1990:NPK

[KASH90] Saad M. Kalipha, Jafar Wadi Abdul-Sada, and Hussain Ali Hussain. New public-key cryptosystem. *International Journal of Systems Science*, 21(1): 205–215, 1990. CODEN IJSYA9. ISSN 0020-7721.

Katzan:1977:SDE

[Kat77] Harry Katzan, Jr. *The Standard Data Encryption Algorithm*. Petrocelli Books, New York, NY, USA, 1977. ISBN 0-89433-016-0. viii + 134 pp. LCCN QA76.9 .A25K37.

Katsikas:1997:CMS

[Kat97] Sokratis Katsikas, editor. *Communications and multimedia security: volume 3: IFIP Joint TC6/TC11 Working Conference on Communications and Multimedia Security, 22–23 September 1997, Athens, Greece*. Chapman & Hall on behalf of the International Federation for Information Processing, London, UK, 1997. ISBN 0-412-81770-5. LCCN QA76.9.A25 I464 1997.

Kaufman:1993:RDD

[Kau93] C. Kaufman. RFC 1507: DASS — distributed authentication security service, September 1993. URL `ftp://ftp.internic.net/rfc/rfc1507.txt`; `https://www.math.utah.edu/pub/rfc/rfc1507.txt`. Status: PROPOSED STANDARD.

Kaufman:1996:DWC

[Kau96] Charlie Kaufman. Differential workfactor cryptography. Web site., 1996. URL `http://www.ussrback.com/crypto/nsa/lotus.notes.nsa.backdoor.txt`.

Kawai:1987:LAI

[Kaw87] Satoru Kawai. Local authentication in insecure environments. *Information Processing Letters*, 25(3): 171–174, May 29, 1987.

CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kay:1995:CTE

[Kay95] Jennifer Kay. Cryptanalysis techniques: an example using Kerberos. Research paper CMU-CS-95-115, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA, September 1995. 15 pp. This is a revised version of a report that first appeared in February 1995.

Krishnakumar:1992:HTE

[KB92] Narayanan Krishnakumar and Arthur J. Bernstein. High throughput escrow algorithms for replicated databases. In Yuan [Yua92], pages 175–186. ISBN 1-55860-151-1. LCCN QA76.9.D3 I61 1992. URL `http://www.vldb.org/dblp/db/conf/vldb/KrishnakumarB92.html`.

Krawczyk:1996:HKM

[KBC96] H. Krawczyk, M. Bellare, and R. Canetti. HMAC-MD5: Keyed-MD5 for message authentication. Internet draft draft-ietf-ipsec-hmac-md5-txt.00., March 1996.

Krawczyk:1997:RHK

[KBC97] H. Krawczyk, M. Bellare, and R. Canetti. RFC 2104: HMAC: Keyed-hashing for message authentication, February 1997. URL `ftp://ftp.internic.net/rfc/rfc2104.txt`; `https://www.math.utah.edu/pub/rfc/rfc2104.txt`. Status: INFORMATIONAL.

Klein:1989:STR

[KBD89] Shmuel T. Klein, Abraham Bookstein, and Scott Deerwester. Storing text retrieval systems on CD-ROM. compression and encryption considerations. *ACM Transactions on Information Systems*, 7(3): 230–245, July 1989. CODEN ATISET. ISSN 1046-8188. URL `http://www.acm.org:80`. Special Issue on Research and Development in Information Retrieval.

Karp:1988:SDN

[KBN88] Bennett C. Karp, L. Kirk Barker, and Larry D. Nelson. The Secure Data Network System. *AT&T Technical Journal*, 67(3): 19–27, May 1988. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Kunkelmann:1997:EDV

[KBRS97] T. Kunkelmann, T. Blecher, R. Reinema, and R. Steinmetz. Evaluation of different video encryption methods for a secure multimedia conferencing gateway. *Lecture Notes in Computer*

Science, 1356:75–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kao:1995:ESA

[KC95] I.-Lung Kao and Randy Chow. An efficient and secure authentication protocol using uncertified keys. *Operating Systems Review*, 29(3):14–21, July 1995. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Krajewski:1994:ASC

[KCCT94a] Marjan Krajewski, Jr., John C. Chipchak, David A. Chodorow, and Jonathan T. Trostle. Applicability of smart cards to network user authentication. *Computing Systems*, 7(1):75–89, Winter 1994. CODEN CMSYE2. ISSN 0895-6340.

Krajewski:COMPSYS-7-1-75

[KCCT94b] Marjan Krajewski, Jr., John C. Chipchak, David A. Chodorow, and Jonathan T. Trostle. Applicability of smart cards to network user authentication. *Computing Systems*, 7(1):75–89, Winter 1994. CODEN CMSYE2. ISSN 0895-6340.

Kam:1978:SDS

[KD78] John B. Kam and George I. Davida. A structured design of substitution-permutation encryption network. In *Foundations of secure computation (Workshop, Georgia Inst. Tech., Atlanta, Ga., 1977)*, pages 95–113. Academic Press, New York, NY, USA, 1978.

Kam:1979:SDS

[KD79] John B. Kam and George I. Davida. Structured design of substitution-permutation encryption networks. *IEEE Transactions on Computers*, 28(10):747–753, 1979. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Khinchin:1997:CF

[KE97] Aleksandrë Iiakovlevich Khinchin and Herbert Eagle. *Continued fractions*. Dover Publications, Inc., New York, NY, USA, 1997. ISBN 0-486-69630-8 (paperback). xi + 95 pp. LCCN QA295 .K513 1997.

Keating:1999:PAA

[Kea99] Geoffrey Keating. Performance analysis of AES candidates on the 6805 CPU core. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/

aes. No slides for the conference talk are available.

Kelsey:1999:KSWb

[Kel99] John Kelsey. Key schedule weaknesses in SAFER+. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Kemp:1988:EEF

[Kem88] Elizabeth A. Kemp. Encryption in electronic funds transfer applications. Massey computer science report 88/2, Computer Science Department, Massey University, Palmerston North, NZ, December 1988. 16 pp.

Kemmerer:1989:AEP

[Kem89] Richard A. Kemmerer. Analyzing encryption protocols using formal verification techniques. Technical report TRCS 89-4, Department of Computer Science, College of Engineering, University of California, Santa Barbara, Santa Barbara, CA, USA, 1989. 23 pp.

Kemppainen:1999:DMM

[Kem99] H. Kemppainen. Designing a mediator for managing relationships between distributed objects. *Lecture Notes in Computer Science*, 1580:253–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kent:1993:IPE

[Ken93] Stephen T. Kent. Internet privacy enhanced mail. *Communications of the Association for Computing Machinery*, 36(8): 48–60, August 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/163390.html.

Kent:1995:PCW

[Ken95] Peter Kent. *PGP companion for Windows: easy point-&-click encryption for your electronic information.* Ventana Press, Chapel Hill, NC, USA, 1995. ISBN 1-56604-304-2. xx + 172 pp. LCCN QA76.9.A25 K46 1995.

Kerr:1975:PIC

[Ker75] Douglas S. Kerr, editor. *Proceedings of the International Conference on Very Large Data Bases, Framingham, MA, USA, September 22–24, 1975.* ACM

Press, New York, NY 10036, USA, 1975. ISBN ???? ISSN 0278-2596. LCCN QA76.9.D3 I55 1975. US$15.00.

Kerr:1989:SNM

[Ker89] S. Kerr. A secret no more (security and encryption). *Datamation*, 35(13):53–55, July 1989. CODEN DTMNAT. ISSN 0011-6963.

Knoble:1979:EOW

[KFB79] H. D. Knoble, C. Forney, Jr., and F. S. Bader. An efficient one-way enciphering algorithm. *ACM Transactions on Mathematical Software*, 5(1):97–107, March 1979. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Kesdogan:1996:LMS

[KFJP96] D. Kesdogan, H. Federrath, A. Jerichow, and A. Pfitzmann. Location management strategies increasing privacy in mobile communication. In Katsikas and Gritzalis [KG96], pages 39–48. ISBN 0-412-78120-4. LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054145.html`.

Kit:1993:DDI

[KG93] Fung Ka Kit and Athula Ginige, editors. *DICTA-93: digital image computing: techniques and applications: conference proceedings, 8–10 December 1993, Macquarie University, Sydney, NSW, Australia*. Australian Pattern Recognition Society, Sydney, NSW, Australia, 1993. ISBN 0-646-16522-4. LCCN ???? Two volumes. Second biennial conference of the Australian Pattern Recognition Society.

Klapper:1995:CBA

[KG95] Andrew Klapper and Mark Goresky. Cryptanalysis based on 2-adic rational approximation. *Lecture Notes in Computer Science*, 963: 262–273, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Katsikas:1996:ISS

[KG96] Sokratis K. Katsikas and Dimitris Gritzalis, editors. *Information systems security: facing the information society of the 21st century: 12th International Information Security Conference, May 21–24 1996, Samos, Greece*. Chapman & Hall, London, UK, 1996. ISBN 0-412-78120-4. LCCN ????

Kravitz:1999:CAC

[KG99] D. W. Kravitz and D. M. Goldschlag. Conditional access concepts and principles. In Franklin [Fra99], pages 158–172. ISBN 3-540-

66362-2 (softcover). LCCN HG1710 .F35 1999.

Kundur:1997:RDI

[KH97] Deepa Kundur and Dimitrios Hatzinakos. Robust digital image watermarking method using wavelet-based fusion. In IEEE [IEE97h], pages 544–547. ISBN 0-8186-8183-7, 0-8186-8184-5 (case). LCCN TK8315 .I16 1997. Three volumes. IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144.

Kundur:1998:DWU

[KH98a] Deepa Kundur and Dimitrios Hatzinakos. Digital watermarking using multiresolution wavelet decomposition. *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing*, 5: 2969–2972, 1998. CODEN IPRODJ. ISSN 0736-7791. IEEE catalog number 98CH36181.

Kunkelmann:1998:VEB

[KH98b] Thomas Kunkelmann and Uwe Horn. Video encryption based on data partitioning and scalable coding — a comparison. *Lecture Notes in Computer Science*, 1483:95–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1483/14830095.htm; http://link.springer-ny.com/link/service/series/0558/papers/1483/14830095.pdf`.

Kharitonov:1993:CHD

[Kha93] Michael Kharitonov. Cryptographic hardness of distribution-specific learning. In ACM [ACM93b], pages 372–381. ISBN 0-89791-591-7. LCCN QA 76.6 A13 1993. URL `http://www.acm.org/pubs/articles/proceedings/stoc/167088/p372-kharitonov/p372-kharitonov.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/167088/p372-kharitonov/`. ACM order no. 508930.

Karaorman:1999:CRJ

[KHB99] M. Karaorman, U. Hoelzle, and J. Bruno. Contractor: a reflective Java library to support design by contract. *Lecture Notes in Computer Science*, 1616:175–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kobara:1996:LVS

[KI96] K. Kobara and H. Imai. Limiting the visible space visual secret sharing schemes and their application to human identification. *Lecture Notes in Computer Science*, 1163:185–??, 1996. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kobara:1997:SSM

[KI97] K. Kobara and H. Imai. Self-synchronised message randomisation method for subliminal channels. In Han et al. [HOQ97], pages 325–334. CODEN LNCSD9. ISBN 3-540-63696-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I554 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064155.html.

Katsumoto:1999:DPL

[KI99] M. Katsumoto and S.-I. Iisaku. Design of the presentation language for distributed hypermedia system. *Lecture Notes in Computer Science*, 1614:375–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kiefer:1998:WMV

[Kie98] K. Kiefer. A weakness of the Menezes–Vanstone cryptosystem. *Lecture Notes in Computer Science*, 1361: 201–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kilian:1988:FCO

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In ACM [ACM88], pages 20–31. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. URL http://www.acm.org/pubs/articles/proceedings/stoc/62212/p20-kilian/p20-kilian.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/62212/p20-kilian/. ACM order no. 508880.

Kim:1993:CLB

[Kim93] Kwangjo Kim. Construction of DES-Like S-boxes based on Boolean functions satisfying the SAC. *Lecture Notes in Computer Science*, 739:59–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kippenhahn:1997:VBG

[Kip97] Rudolf Kippenhahn. *Verschlüsselte Botschaften: Geheimschrift, Enigma und Chipkarte. (German) [Encrypted messages: cryptography, Enigma and smart card].* Rowohlt, Reinbek bei Hamburg, Germany, 1997. ISBN 3-498-03495-2. 362 pp. LCCN ???? DM 45.00.

Kippenhahn:1999:CBH

[Kip99a] Rudolf Kippenhahn. *Code breaking: a history and exploration.* Overlook Press, Woodstock, NY, USA, 1999. ISBN 0-87951-919-3. 283 pp. LCCN Z103 .K5613 1999. Translated from the German original, Verschlüßelte Botschaften, in collaboration with the author, by Ewald Osers.

Kippenhahn:1999:VBG

[Kip99b] Rudolf Kippenhahn. *Verschlüsselte Botschaften: Geheimschrift, Enigma und Chipkarte*, volume 60807 of *rororo rororo-Sachbuch science*. Rowohlt-Taschenbuch-Verl., Reinbek bei Hamburg, second edition, 1999. ISBN 3-499-60807-3. 361 pp. LCCN ????

Kirby:1995:RPK

[Kir95] Jeff Kirby. The RSA public key encryption algorithm and what a business needs to know about it. Thesis (B.S.), California Polytechnic State University, San Luis Obispo, CA, USA, 1995. v + 72 pp.

Kak:1977:SEU

[KJ77] S. C. Kak and N. S. Jayant. On speech encryption using waveform scrambling. *The Bell System Technical Journal*, 56(5):781–808, May–June 1977. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol56/bstj56-5-781.pdf`.

Kocher:1999:DPA

[KJJ99] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In Wiener [Wie99], pages 388–397. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Kurosawa:1995:NBA

[KK95] K. Kurosawa and S. Kageyama. New bound for affine resolvable designs and its application to authentication codes. *Lecture Notes in Computer Science*, 959: 292–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kuwakado:1996:NRT

[KK96] Hidenori Kuwakado and Kenji Koyama. A new RSA-type cryptosystem based on singular cubic curves. In *Applications of finite fields (Egham, 1994)*, volume 59 of *Inst. Math. Appl. Conf. Ser. New Ser.*, pages 99–109. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1996.

Kelm:1997:NK

[KK97] S. Kelm and K. P. Kossakowski. Zur Notwendigkeit der Kryptographie (German) [on the necessity of cryptography]. *Datenschutz und Datensicherheit*, 21(4): 192–196, April 1997. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/062338.html`.

Kunihiro:1998:ECN

[KK98] N. Kunihiro and K. Koyama. Equivalence of counting the number of points on elliptic curve over the ring Z_n and factoring n. *Lecture Notes in Computer Science*, 1403:47–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kommerling:1999:DPT

[KK99a] Oliver Kömmerling and Markus G. Kuhn. Design principles for tamper-resistant Smartcard processors. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL http://www.usenix.org/publications/library/proceedings/smartcard99/kommerling.html.

Koren:1999:ISC

[KK99b] Israel Koren and Peter Kornerup, editors. *14th IEEE Symposium on Computer Arithmetic: proceedings: April 14–16, 1999, Adelaide, Australia*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1999. ISBN 0-7803-5609-8, 0-7695-0116-8, 0-7695-0118-4. ISSN 1063-6889. LCCN QA76.6 .S887 1999. URL http://computer.org/conferen/home/arith/; http://www.ecs.umass.edu/ece/arith14/program.html. IEEE Computer Society Order Number PR00116. IEEE Order Plan Catalog Number 99CB36336.

Koshelev:1999:EAM

[KKL99] Misha Koshelev, Vladik Kreinovich, and Luc Longpré. Encryption algorithms made natural. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 31(4):50–51, December 1999. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Kurosawa:1991:GPK

[KKOT91] Kaoru Kurosawa, Yutaka Katayama, Wakaha Ogata, and Shigeo Tsujii. General public key residue cryptosystems and mental poker protocols. *Lecture Notes in Computer Science*, 473:374–388, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730374.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730374.pdf.

Kabatianskii:1997:DSS

[KKS97] G. Kabatianskii, E. Krouk, and B. Smeets. A digital signature scheme based on random error-correcting codes. *Lecture Notes in*

Computer Science, 1355: 161–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kramer:1999:FCD

[KKW99] K.-D. Kramer, J. Kirschner, and S. Woehlbier. Fuzzy-control design tool for low-cost microcontrollers (FHFC-Tool). *Lecture Notes in Computer Science*, 1625:88–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kothari:1984:CMW

[KL84] S. Kothari and S. Lakshmivarahan. On the concealability of messages by the Williams public-key encryption scheme. *Computers and Mathematics with Applications*, 10(1):15–24, 1984. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Kilian:1994:FKE

[KL94] Joseph J. Kilian and T. Leighton. Failsafe key escrow. Technical report MIT/LCS/TR-636, Massachusetts Institute of Technology. Laboratory for Computer Science, Cambridge, MA, USA, August 1994. 19 pp.

Kilian:1995:FCR

[KL95a] Joe Kilian and Tom Leighton. Fair cryptosystems, revisited. *Lecture Notes in Computer Science*, 963: 208–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630208.htm; http://link.springer-ny.com/link/service/series/0558/papers/0963/09630208.pdf`.

Knudsen:1995:NAA

[KL95b] L. R. Knudsen and X. Lai. New attacks on all double block length hash functions of hash rate 1, including the parallel-DM. *Lecture Notes in Computer Science*, 950: 410–418, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Klein:1990:FCS

[Kle90] Daniel Klein. Foiling the cracker: a survey of, and improvements to, password security. In USENIX Association [USE90], pages 5–14. LCCN QA 76.9 A25 U55 1990.

Kannan:1988:PFN

[KLL88] R. Kannan, A. K. Lenstra, and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Mathematics of Computation*, 50(181):235–250, January 1988. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Klupsch:1999:ARR

[KLZL99] M. Klupsch, M. Lueckenhaus, C. Ziert, and I. Laptev. Agile RoboCuppers: RoboCup team description. *Lecture Notes in Computer Science*, 1604: 446–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kurosawa:1988:CSP

[KM88] K. Kurosawa and K. Matsu. Cryptographically secure pseudorandom sequence generator based on reciprocal number cryptosystem. *Electronics Letters*, 24(1): 16–17, January 7, 1988. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8134`.

Kurak:1992:CNI

[KM92] C. Kurak and J. McHugh. A cautionary note on image downgrading. In IEEE [IEE92b], pages 153–159. ISBN 0-8186-3115-5 (paperback), 0-8186-3116-3 (microfiche), 0-8186-3117-1 (casebound). LCCN QA76.9.A25 C6375 1992. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1012.html`. IEEE Computer Society Press order number 3115. IEEE catalog number 92TH04070-5.

Kang:1993:PRR

[KM93] M. H. Kang and I. S. Moskowitz. A pump for rapid, reliable, secure communications. In ACM [ACM93a], pages 118–129. ISBN 0-89791-629-8. LCCN QA76.9.A25 A26 1993. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/031218.html`.

Kim:1996:ACA

[KM96a] Kwangjo Kim and Tsutomu Matsumoto, editors. *Advances in cryptology–ASIACRYPT '96: International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3–7, 1996: proceedings*, volume 1163 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-61872-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5553 1996.

Knudsen:1996:IDA

[KM96b] L. Knudsen and W. Meier. Improved differential attacks on RC5. In Koblitz [Kob96], pages 171–183. CODEN LNCSD9. ISBN 3-540-61512-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1996. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1109.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1109. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Kosuda:1997:SED

[KM97] Koji Kosuda and Tsutomu Matsumoto. A strength evaluation of the Data Encryption Standard. IMES discussion paper 97-E-5, Institute for Monetary and Economic Studies, Bank of Japan, Tokyo, Japan, 1997. 128 pp.

Kaksonen:1998:OMC

[KM98a] R. Kaksonen and P. Maehoenen. Object modeling of cryptographic algorithms with UML 193. *Lecture Notes in Computer Science*, 1438:193–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kaufman:1998:DWF

[KM98b] C. W. Kaufman and S. M. Matyas. Differential work factor cryptography method and system. US Patent 5,764,772., June 9, 1998.

Knudsen:1998:SMD

[KM98c] Lars R. Knudsen and Keith M. Martin. In search of multiple domain key recovery. *Journal of Computer Security*, 6(4):219–235, ???? 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kasahara:1999:NPK

[KM99a] Masao Kasahara and Yasuyuki Murakami. New public-key cryptosystems based on arithmetic in integer ring. *Mem. Fac. Engrg. Design Kyoto Inst. Tech. Ser. Sci. Tech.*, 48:43–57 (2000), 1999. ISSN 0911-0305.

Knudsen:1999:CIS

[KM99b] L. R. Knudsen and W. Meier. Cryptanalysis of an identification scheme based on the permuted perceptron problem. *Lecture Notes in Computer Science*, 1592:363–??,

1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kohlas:1999:RAP

[KM99c] Reto Kohlas and Ueli Maurer. Reasoning about public-key certification: On bindings between entities and public keys. In Franklin [Fra99], pages 86–103. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1648/16480086.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1648/16480086.pdf`.

Koscielny:1999:QBP

[KM99d] Czesław Kościelny and Gary L. Mullen. A quasigroup-based public-key cryptosystem. *Int. J. Appl. Math. Comput. Sci.*, 9(4):955–963, 1999. ISSN 1641-876X.

Kanda:1998:ECC

[KMA+98] Masayuki Kanda, Shiho Moriai, Kazumaro Aoki, Hiroki Ueda, Miyako Ohkubo, Youichi Takashima, Kazuo Ohta, and Tsutomu Matsumoto. E2 — a candidate cipher for AES. In National Institute of Standards and Technology [Nat98], page 89. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf1/e2-slides.pdf`. Only the slides for the conference talk are available.

Kobayashi:1999:FEC

[KMKH99] T. Kobayashi, H. Morita, K. Kobayashi, and F. Hoshino. Fast elliptic curve algorithm combining Frobenius map and table reference to adapt to higher characteristic. *Lecture Notes in Computer Science*, 1592: 176–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Konheim:1980:ICP

[KMM+80] Alan G. Konheim, Marian H. Mack, Robert K. McNeill, Bryant Tuckerman, and Gerald Waldbaum. The IPS cryptographic programs. *IBM Systems Journal*, 19(2): 253–283, 1980. CODEN IBMSA7. ISSN 0018-8670.

Koyama:1991:NPK

[KMOV91] Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, and Scott A. Vanstone. New public-key schemes based on elliptic curves over the ring Z_n. *Lecture Notes in Computer Science*, 576: 252–266, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/`

link/service/series/0558/bibs/0576/05760252.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760252.pdf.

Kande:1999:AUD

[KMPS99] M. Mancona Kande, S. Mazaher, O. Prnjat, and L. Sacks. Applying UML to design an inter-domain service management application. *Lecture Notes in Computer Science*, 1618:200–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Karn:1995:REC

[KMS95a] P. Karn, P. Metzger, and W. Simpson. RFC 1829: The ESP DES-CBC transform, August 1995. URL ftp://ftp.internic.net/rfc/rfc1829.txt; https://www.math.utah.edu/pub/rfc/rfc1829.txt. Status: PROPOSED STANDARD.

Karn:1995:RET

[KMS95b] P. Karn, P. Metzger, and W. Simpson. RFC 1851: The ESP triple DES transform, September 1995. URL ftp://ftp.internic.net/rfc/rfc1851.txt; https://www.math.utah.edu/pub/rfc/rfc1851.txt. Status: EXPERIMENTAL.

Kohl:1993:RKN

[KN93] J. Kohl and C. Neuman. RFC 1510: The Kerberos Network Authentication Service (V5), September 1993. URL ftp://ftp.internic.net/rfc/rfc1510.txt; https://www.math.utah.edu/pub/rfc/rfc1510.txt. Status: PROPOSED STANDARD.

Knoble:1979:AEO

[Kno79] H. D. Knoble. Algorithm 536: An efficient one-way enciphering algorithm [Z]. *ACM Transactions on Mathematical Software*, 5 (1):108–111, March 1979. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Kohl:1994:EKA

[KNT94] John T. Kohl, B. Clifford Neuman, and Theodore Y. Ts'o. The evolution of the Kerberos authentication service. ISI reprint ISI/RS-94-412, University of Southern California, Information Sciences Institute, Marina del Rey, CA, USA, 1994. 17 pp. Reprinted, with permission from Distributed Open Systems, Editors F. M. T. Brazier and D. Johansen, pp. 78–94, 1994.

Knuth:1969:SNM

[Knu69a] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Com-*

puter Programming. Addison-Wesley, Reading, MA, USA, 1969. ISBN 0-201-03802-1. xi + 624 pp. LCCN QA76.5 .K57. US$19.75. See pages 248–250.

Knuth:1969:SA

[Knu69b] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, 1969. ISBN 0-201-03802-1. xi + 624 pp. LCCN QA76.5 .K57. US$19.75.

Knuth:1973:FA

[Knu73] Donald E. Knuth. *Fundamental Algorithms*, volume 1 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, second edition, 1973. ISBN 0-201-03809-9. xxi + 634 pp. LCCN QA76.6 .K641 1973.

Knuth:1980:DLC

[Knu80] Donald E. Knuth. Deciphering a linear congruential encryption. Report 024800, Department of Computer Science, Stanford University, Stanford, CA, USA, 1980.

Knuth:1985:DLC

[Knu85] Donald E. Knuth. Deciphering a linear congruential encryption. *IEEE Transactions on Information Theory*, IT-31(1):49–52, January 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). Russian translation, to appear.

Knuth:1987:CT

[Knu87] Donald E. Knuth. *N*-ciphered texts. *Word Ways*, 20(??):173–174, 191–192, 1987. ISSN 0043-7980.

Knudsen:1992:CL

[Knu92] Lars Ramkilde Knudsen. Cryptanalysis of LOKI. Technical Report DAIMI PB-403, Computer Science Department, Aarhus University, Århus, Denmark, July 1992. 17 pp.

Knudsen:1993:CLb

[Knu93a] L. R. Knudsen. Cryptanalysis of LOKI91. *Lecture Notes in Computer Science*, 718:196–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1993:ICS

[Knu93b] L. R. Knudsen. Iterative characteristics of DES and s^2-DES. *Lecture Notes in Computer Science*, 740: 497–511, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1993:CLc

[Knu93c] Lars Ramkilde Knudsen. Cryptanalysis of LOKI. *Lecture Notes in Computer*

Science, 739:22–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1993:CLa

[Knu93d] Lars Ramkilde Knudsen. Cryptanalysis of LOKI91. Technical report DAIMI PB-440, Computer Science Department, Aarhus University, Århus, Denmark, 1993. 18 pp.

Knudsen:1994:PSF

[Knu94a] L. Knudsen. Practically secure Feistel ciphers. *Lecture Notes in Computer Science*, 809:211–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1994:BCA

[Knu94b] L. R. Knudsen. *Block Ciphers — Analysis, Design and Applications*. Thesis (Ph.D.), Aarhus University, Aarhus, Denmark, 1994.

Knudsen:1995:NPW

[Knu95] L. R. Knudsen. New potentially weak' keys for DES and LOKI. *Lecture Notes in Computer Science*, 950:419–424, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1998:JC

[Knu98a] Jonathan B. Knudsen. *Java Cryptography*. 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, May 1998. ISBN 1-56592-402-9. xvi + 344 pp. LCCN QA76.73.J38 K59 1999. US$29.95. URL `http://www.ora.com/catalog/javacrypt/`.

Knudsen:1998:BCS

[Knu98b] L. R. Knudsen. Block ciphers — a survey. *Lecture Notes in Computer Science*, 1528:18–48, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1998:DBC

[Knu98c] L. R. Knudsen. DEAL — a 128-bit block cipher. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, February 1998.

Knudsen:1999:STA

[Knu99a] L. Knudsen. Some thoughts on the AES process. Comment submitted to NIST., April 1999.

Knudsen:1999:CBC

[Knu99b] L. R. Knudsen. Contemporary block ciphers. *Lecture Notes in Computer Science*, 1561:105–126, 1999. CODEN LNCSD9. ISSN

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

Knudsen:1999:FSE

[Knu99c] Lars Knudsen, editor. *Fast software encryption: 6th International Workshop, FSE'99, Rome, Italy, March 24–26, 1999: proceedings*, volume 1636 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Kurosawa:1995:CIS

[KO95a] K. Kurosawa and K. Okada. Combinatorial interpretation of secret sharing schemes. *Lecture Notes in Computer Science*, 917: 55–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kurosawa:1995:CBA

[KO95b] Kaoru Kurosawa and Satoshi Obana. Combinatorial bounds for authentication codes with arbitration. *Lecture Notes in Computer Science*, 921:289–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210289.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0921/09210289.pdf`.

Kurosawa:1996:CLB

[KO96] Kaoru Kurosawa and Koji Okada. Combinatorial lower bounds for secret sharing schemes. *Information Processing Letters*, 60 (6):301–304, December 23, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kurosawa:1997:CLB

[KO97] Kaoru Kurosawa and Koji Okada. Combinatorial lower bounds for secret sharing schemes. *Information Processing Letters*, 60(6):301–304, January 31, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Koblitz:1987:CNT

[Kob87a] Neal Koblitz. *A course in number theory and cryptography*, volume 114 of *Graduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-96576-9. 208 pp. LCCN QA241 .K6721 1987. US$29.80.

Koblitz:1987:ECC

[Kob87b] Neal Koblitz. Elliptic curve cryptosystems. *Math-*

ematics of Computation, 48(177):203–209, January 1987. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Koblitz:1990:FJS

[Kob90] Neal Koblitz. A family of Jacobians suitable for discrete log cryptosystems. *Lecture Notes in Computer Science*, 403:94–99, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Koblitz:1991:CCG

[Kob91a] Neal Koblitz. CM-curves with good cryptographic properties. *Lecture Notes in Computer Science*, 576: 279–287, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Koblitz:1991:CEC

[Kob91b] Neal Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. *Lecture Notes in Computer Science*, 537:156–167, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Koblitz:1991:JSI

[Kob91c] Neal Koblitz. Jacobi sums, irreducible zeta-polynomials, and cryptography. *Bulletin canadien de mathématiques = Canadian Mathematical Bulletin*, 34(??):229–235, ???? 1991. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Koblitz:1994:CNT

[Kob94] Neal Koblitz. *A Course in Number Theory and Cryptography*, volume 114 of *Graduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 1994. ISBN 0-387-94293-9, 0-387-96576-9 (New York), 3-540-96576-9 (Berlin). x + 235 pp. LCCN QA241 .K672 1994.

Koblitz:1996:ACC

[Kob96] Neal Koblitz, editor. *Advances in cryptology, CRYPTO '96: 16th annual international cryptology conference, Santa Barbara, California, USA, August 18–22, 1996: proceedings*, volume 1109 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-61512-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1996. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1109.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&`

issn=0302-9743&volume=1109. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Kobayashi:1997:DWH

[Kob97] M. Kobayashi. Digital watermarking: Historical roots. IBM Research Report RT0199, IBM Japan, Tokyo, Japan (??), April 1997. ??–?? pp. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073142.html.

Koblitz:1998:C

[Kob98a] N. Koblitz. Crypto '96. *Lecture Notes in Computer Science*, 1440:207–214, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Koblitz:1998:AAC

[Kob98b] Neal Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and computation in mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-63446-0 (hardcover). ISSN 1431-1550. ix + 206 pp. LCCN QA268 .K585 1998. With an appendix on hyperelliptic curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato.

Koblitz:1998:ECI

[Kob98c] Neal Koblitz. An elliptic curve implementation of the finite field digital signature algorithm. *Lecture Notes in Computer Science*, 1462:327–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620327.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620327.pdf.

Kobara:1999:PMA

[Kob99] Kazukuni Kobara. Pseudorandomness and maximum average of differential probability of block ciphers with SPN-structures like E2. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Kochanski:1989:HSI

[Koc89] Martin Kochanski. How safe is it? (computer security). *BYTE Magazine*, 14(6):257–264, June 1989. CODEN BYTEDJ. ISSN 0360-5280.

Koc:1994:HSR

[Koç94] Çetin Kaya Koç. High-speed RSA implementation. Technical report TR 201, RSA Data Security, Inc., Redwood City, CA, USA, November 1994. 73 pp. URL ftp://ftp.rsasecurity.com/pub/pdfs/tr201.pdf. Version 2.0.

Kocher:1995:CDR

[Koc95] P. Kocher. Cryptanalysis of Diffie–Hellman, RSA, DSS, and other cryptosystems using timing attacks. In Coppersmith [Cop95d], pages 171–183. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=963. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Koc:1996:RHI

[Koç96a] Çetin Kaya Koç. RSA hardware implementation. Technical report TR-801, RSA Data Security, Inc., Redwood City, CA, USA, April 19, 1996. ii + 33 pp. URL ftp://ftp.rsasecurity.com/pub/ps/tr801.pdf; ftp://ftp.rsasecurity.com/pub/ps/tr801.ps. Version 1.0.

Kocher:1996:TAI

[Koc96b] Paul C. Kocher. Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems. *Lecture Notes in Computer Science*, 1109:104–113, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090104.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090104.pdf.

Kocher:1999:B

[Koc99] Paul C. Kocher. Breaking DES. *CryptoBytes*, 4(2):1, 3–5, Winter 1999. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n2.pdf.

Koeune:1999:CRI

[Koe99] François Koeune. cAESar results: Implementation of four AES candidates on two smart cards. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Kohl:1990:UEK

[Koh90] John T. Kohl. The use of encryption in Kerberos for network authentication (invited). *Lecture Notes in Computer Science*, 435: 35–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350035.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350035.pdf.

Kolata:1977:NCC

[Kol77] Gina Bari Kolata. News and comment: Computer encryption and the National Security Agency connection. *Science*, 197(4302): 438–440, July 29, 1977. CODEN SCIEAS. ISSN 0036-8075 (print), 1095-9203 (electronic). URL http://science.sciencemag.org/content/197/4302/438/.

Koland:1995:SSH

[Kol95] Cordell Koland. Sharing or Segregating Host Resources. *Open Computing*, 12(2):65–??, February 1995. CODEN OPCOEB. ISSN 1078-2370.

Konheim:1981:CP

[Kon81] Alan G. Konheim. *Cryptography, a primer*. John Wiley and Sons, Inc., New York, NY, USA, 1981. ISBN 0-471-08132-9. xiv + 432 pp. LCCN Z103 .K66 1981. A Wiley-interscience publication.

Konheim:1985:CAE

[Kon85] Alan G. Konheim. Cryptanalysis of ADFGVX encipherment systems (extended abstract). In Blakley and Chaum [BC85], pages 339–341. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=339. CRYPTO 84: a Workshop on the Theory and Application of

Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Konheim:1989:RMC

[Kon89] Alan G. Konheim. Reviews: *Mathematical Cryptology for Computer Scientists and Mathematicians*, by Wayne Patterson; *A Course in Number Theory and Cryptography*, by Neal Koblitz. *American Mathematical Monthly*, 96(4):374–375, April 1989. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Kong:1995:DES

[Kon95] Michael M. Kong. DCE: An environment for secure client/server computing. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 46(6):6–15, December 1995. CODEN HPJOAX. ISSN 0018-1153. URL http://www.hp.com/hpj/95dec/dec95_6t.pdf; http://www.hp.com/hpj/toc-12-95.html.

Koopman:1986:OES

[Koo86] Raymond F. Koopman. The orders of equidistribution of subsequences of some asymptotically random sequences. *Communications of the Association for Computing Machinery*, 29(8):802–806, August 1986. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/6431.html.

Kurosawa:1995:TIK

[KOO95a] K. Kurosawa, S. Obana, and W. Ogata. t-cheater identifiable (k, n) threshold secret sharing schemes. *Lecture Notes in Computer Science*, 963:410–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kurosawa:1995:CIT

[KOO95b] Kaoru Kurosawa, Satoshi Obana, and Wakaha Ogata. t-cheater identifiable (k, n) threshold secret sharing schemes. *Lecture Notes in Computer Science*, 963:410–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630410.htm; http://link.springer-ny.com/link/service/series/0558/papers/0963/09630410.pdf.

Koops:1997:CRE

[Koo97] Bert-Jaap Koops. Crypto

regulation in Europe. Some key trends and issues. *Computer Networks and ISDN Systems*, 29(15):1823–1831, November 1, 1997. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/comnet/cas_sub/browse/browse.cgi?year=1997&volume=29&issue=15&aid=1773.

Kopooshian:1997:DCE

[Kop97] Hrag H. Kopooshian. Data compression and encryption. Thesis (M.S.), California State University, Northridge, Northridge, CA, USA, 1997. vi + 127 pp.

Kornerup:1993:HRM

[Kor93] Peter Kornerup. High-radix modular multiplication for cryptosystems. In Swartzlander, Jr. et al. [SIJ93], pages 277–283. ISBN 0-7803-1401-8 (softbound), 0-8186-3862-1 (casebound), 0-8186-3861-3 (microfiche). ISSN 0018-9340 (print), 1557-9956 (electronic). LCCN QA 76.9 C62 S95 1993. URL http://www.acsel-lab.com/arithmetic/arith11/papers/ARITH11_Kornerup.pdf. IEEE Transactions on Computers **43(8)**, 1994.

Korner:1996:PC

[Kör96] T. W. (Thomas William) Körner. *The Pleasures of Counting*. Cambridge University Press, Cambridge, UK, 1996. ISBN 0-521-56823-4 (paperback), 0-521-56087-X (hardback). x + 534 pp. LCCN QA93 .K65 1996. URL http://www.loc.gov/catdir/description/cam029/97108334.html; http://www.loc.gov/catdir/toc/cam027/97108334.html.

Koscielny:1983:PRD

[Kos83] Czeslaw Koscielny. *Programowa realizacja dzialan w cialach skonczonych do zastosowan w technice kodowania korekcyjnego i kryptografii*, volume 61. 11 of *Prace naukowe Instytutu Cybernetyki Technicznej Politechniki Wroclawskiej; Seria Monografie*. Wydawn. Politechniki Wroclawskiej, Wroclaw, Poland, 1983. ISBN ???? ISSN 0324-9786. 115 pp. LCCN QA76.9.A251 K6 1983. zl93.00. Title on p. [2] of cover: A software approach to computing in finite fields with applications to error-correcting coding technique and cryptography. Summary in English and Russian; legends and table of contents also in English. Bibliography: p. 109–110.

Kurosawa:1994:NSS

[KOS+94] Kaoru Kurosawa, Koji Okada, Keiichi Sakano, Wakaha Ogata, and Shigeo Tsujii. Nonperfect secret sharing schemes and matroids. *Lecture Notes in Computer Science*, 765: 126–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650126.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650126.pdf`.

Koshiba:1997:CLT

[Kos97] T. Koshiba. Computational learning theoretic cryptanalysis of language theoretic cryptosystems. *Lecture Notes in Computer Science*, 1334:28–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Koshiba:1999:UPN

[Kos99] Takeshi Koshiba. Unpredictability of pseudorandom number generators on public key cryptosystems with random inputs. *Sūrikaisekikenkyūsho Kōkyūroku*, 1093:162–167, 1999. Models of computation and algorithms (Japanese) (Kyoto, 1999).

Kothari:1985:GLT

[Kot85] S. C. Kothari. Generalized linear threshold scheme. In Blakley and Chaum [BC85], pages 231–241. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=231`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Kurosawa:1995:LEAa

[KOT95a] Kaoru Kurosawa, Koji Okada, and Shigeo Tsujii. Low exponent attack against elliptic curve RSA. *Information Processing Letters*, 53(2):77–83, January 27, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kurosawa:1995:LEAb

[KOT95b] Kaoru Kurosawa, Koji Okada, and Shigeo Tsujii. Low exponent attack against elliptic curve RSA. *Lecture Notes in Computer Science*, 917:376–383, 1995. CODEN LNCSD9. ISSN

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

Koyama:1982:CUM

[Koy82a] Kenji Koyama. A cryptosystem using the master key for multi-address communication. *Systems-Comput.-Controls*, 13(5): 36–46 (1983), 1982. CODEN SYCCBB. ISSN 0096-8765.

Koyama:1982:MKR

[Koy82b] Kenji Koyama. A master key for the RSA public-key cryptosystem. *Systems-Comput.-Controls*, 13(1): 63–70 (1983), 1982. CODEN SYCCBB. ISSN 0096-8765.

Koyama:1983:MKR

[Koy83] Kenji Koyama. A master key for the Rabin's public-key cryptosystem. *Systems-Comput.-Controls*, 14(6): 49–57 (1984), 1983. CODEN SYCCBB. ISSN 0096-8765.

Koyama:1995:FRT

[Koy95] Kenji Koyama. Fast RSA-type schemes based on singular cubic curves $y^2 + axy \equiv x^3 \pmod{n}$. *Lecture Notes in Computer Science*, 921:329–340, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210329.htm; http://link.springer-ny.com/link/service/series/0558/papers/0921/09210329.pdf.

Kozaczuk:1984:EHGa

[Koz84a] Władysław Kozaczuk. *Enigma: how the German machine cipher was broken, and how it was read by the Allies in World War Two*. Arms and Armour, London, UK, 1984. ISBN 0-85368-640-8. xiv + 348 pp. LCCN D810.C88 K6813 1984b. Translation of: W kregu Enigmy.

Kozaczuk:1984:EHGb

[Koz84b] Władysław Kozaczuk. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*. Foreign intelligence book series. University Publications of America, Frederick, MD, USA, 1984. ISBN 0-89093-547-5. xiv + 348 pp. LCCN D810.C88 K6813 1984. US$24.00. Edited and translated by Christopher Kasparek, from the original Polish edition, *W kręgu Enigma*, Książka i Wiedza, Warsaw, 1979.

Kozen:1996:RSS

[Koz96] Dexter Kozen. Rational spaces and set constraints. *Theoretical Computer Science*, 167(1–2):73–94, October 30, 1996. CODEN

TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1996&volume=167&issue=1-2&aid=2272.

Kim:1989:PRP

[KP89] Su Hee Kim and Carl Pomerance. The probability that a random probable prime is composite. *Mathematics of Computation*, 53(188):721–741, October 1989. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Kwan:1993:GPT

[KP93] Matthew Kwan and Josef Pieprzyk. A general purpose technique for locating key scheduling weaknesses in DES-like cryptosystems. *Lecture Notes in Computer Science*, 739:237–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Krajicek:1995:SCC

[KP95] J. Krajicek and P. Pudlak. Some consequences of cryptographical conjectures for S012 and EF. *Lecture Notes in Computer Science*, 960:210–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1996:HFB

[KP96a] L. Knudsen and B. Preneel. Hash functions based on block ciphers and quaternary codes. *Lecture Notes in Computer Science*, 1163:77–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1996:DSK

[KP96b] Lars R. Knudsen and Torben P. Pedersen. On the difficulty of software key escrow. *Lecture Notes in Computer Science*, 1070:237–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700237.htm; http://link.springer-ny.com/link/service/series/0558/papers/1070/10700237.pdf.

Knudsen:1997:FSH

[KP97] Lars Ramkilde Knudsen and Bart Preneel. Fast and secure hashing based on codes. *Lecture Notes in Computer Science*, 1294:485–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940485.htm;

http://link.springer-ny.com/link/service/series/0558/papers/1294/12940485.pdf.

Kilian:1998:IE

[KP98] Joe Kilian and Erez Petrank. Identity escrow. *Lecture Notes in Computer Science*, 1462:169–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620169.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620169.pdf.

Kaps:1999:FIF

[KP99a] J.-P. Kaps and C. Paar. Fast DES implementation for FPGAs and its application to a universal key-search machine. *Lecture Notes in Computer Science*, 1556:234–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Koc:1999:CHE

[KP99b] Cetin K. Koc and Christof Paar, editors. *Cryptographic hardware and embedded systems: First International Workshop, CHES '99, Worchester, MA, USA, August 1999: proceedings*, volume 1717 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66646-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1717.

Kipnis:1999:UOV

[KPG99] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced oil and vinegar signature schemes. *Lecture Notes in Computer Science*, 1592:206–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Karhumaeki:1999:CSI

[KPR99] J. Karhumaeki, W. Plandowski, and W. Rytter. The compression of subsegments of images described by finite automata. *Lecture Notes in Computer Science*, 1645:186–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kaliski:1994:FBC

[KR94a] B. Kaliski and M. Robshaw. Fast block cipher proposal. *Lecture Notes in Computer Science*, 809:33–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kaliski:1994:LCU

[KR94b] Burton S. Kaliski Jr. and Matthew J. B. Robshaw. Linear cryptanalysis using multiple approximations. In Desmedt [Des94b], pages 26–39. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390026.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390026.pdf.

Kushilevitz:1994:RRT

[KR94c] Eyal Kushilevitz and Adi Rosén. A randomness-rounds tradeoff in private computation. In Desmedt [Des94b], pages 397–410. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390397.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390397.pdf.

Kaliski:1995:LCU

[KR95a] B. S. Kaliski and M. J. B. Robshaw. Linear cryptanalysis using multiple approximations and FEAL. *Lecture Notes in Computer Science*, 1008:249–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kaliski:1995:MAM

[KR95b] Burt Kaliski and Matt Robshaw. Message authentication with MD5. *CryptoBytes*, 1(1):5–8, Spring 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n1.pdf.

Kaliski:1995:SUR

[KR95c] Burt Kaliski and Matt Robshaw. The secure use of RSA. *CryptoBytes*, 1(3):7–13, Autumn 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf.

Kaliski:1996:MEW

[KR96a] Burton S. Kaliski, Jr. and M. J. B. Robshaw. Algorithm alley: Multiple encryption: Weighing security and performance. *Dr. Dobb's Journal of Software Tools*, 21(1):123, 124, 126, 127, January 1996. CODEN DDJOEB. ISSN 1044-789X.

Kilian:1996:HPA

[KR96b] J. Kilian and P. Rogaway. How to protect DES against exhaustive key search. In Koblitz [Kob96], pages 252–?? CODEN LNCSD9. ISBN 3-540-61512-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1996. URL http://wwwcsif.cs.ucdavis.edu/~rogaway. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Knudsen:1996:NAL

[KR96c] L. R. Knudsen and M. J. B. Robshaw. Non-linear approximations in linear cryptanalysis. *Lecture Notes in Computer Science*, 1070:224–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kankanhalli:1998:CBW

[KR98] M. S. Kankanhalli and R. K. R. Ramakrishnan. Content based watermarking of images. In Effelsberg and Smith [ES98], pages 61–70. ISBN 1-58113-036-8. LCCN QA76.575.A36 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073139.html. ACM order number 43398.

Knudsen:1999:DFC

[KR99a] L. R. Knudsen and V. Rijmen. On the decorrelated fast cipher (DFC) and its theory. In Knudsen [Knu99c], pages 81–94. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Kolliopoulos:1999:NLT

[KR99b] S. G. Kolliopoulos and S. Rao. A nearly linear-time approximation scheme for the Euclidean k-median problem. *Lecture Notes in Computer Science*, 1643: 378–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Krause:1984:DEI

[Kra84] Lothar Krause. Data encryption in ISO, the international organization for standardization. *Computers and Security*, 3(3):234–236, August 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404884900452.

Kranakis:1986:PC

[Kra86] Evangelos Kranakis. *Primality and cryptography*. Wiley-Teubner series in computer science. John Wiley and Sons, Inc., New York, NY, USA, 1986. ISBN 0-471-90934-3. xv + 235 pp. LCCN TK5102.5 .K661 1986. US$38.00.

Krawczyk:1990:HPC

[Kra90] Hugo Krawczyk. How to predict congruential generators. *Lecture Notes in Computer Science*, 435: 138–153, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350138.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350138.pdf.

Kravitz:1993:DSA

[Kra93] D. W. Kravitz. Digital signature algorithm. US Patent No. 5,231,668A., July 26, 1993. URL https://www.google.com/patents/US5231668. Patent filed 26 July 1991.

Krawczyk:1994:SSM

[Kra94a] H. Krawczyk. Secret sharing made short. In Stinson [Sti94], pages 136–146. CODEN LNCSD9. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1993. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0773.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=773.

Krawczyk:1994:LBH

[Kra94b] Hugo Krawczyk. LFSR-based hashing and authentication. In Desmedt [Des94b], pages 129–139. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390129.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390129.pdf.

Krawczyk:1995:NHF

[Kra95] Hugo Krawczyk. New hash functions for message authentication. *Lecture Notes in Computer Science*, 921: 301–310, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210301.htm; http://link.springer-ny.com/link/service/series/0558/papers/0921/09210301.pdf.

Krawczyk:1998:ACC

[Kra98] Hugo Krawczyk, editor. *Advances in cryptology —*

CRYPTO '98: 18th Annual International Cryptology Conference, Santa Barbara, California, USA August 23–27, 1998 proceedings, volume 1462 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-64892-5 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1998. Sponsored by the International Association for Cryptologic Reseach, (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department, University of California, Santa Barbara (UCSB).

Krawczyk:1999:BCC

[Kra99] H. Krawczyk. Blinding of credit card numbers in the SET protocol. In Franklin [Fra99], pages 17–28. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Kesdogan:1998:DTP

[KRJ98] D. Kesdogan, P. Reichl, and K. Junghärtchen. Distributed temporary pseudonyms: a new approach for protecting location information in mobile communication networks. In Quisquater et al. [Q+98], pages 295–312. ISBN 3-540-65004-0. LCCN QA267.A1 L43 no.1485. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073140.html.

Knudsen:1998:DSR

[KRRR98] L. R. Knudsen, V. Rijmen, R. L. Rivest, and M. J. B. Robshaw. On the design and security of RC2. *Lecture Notes in Computer Science*, 1372:206–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kumar:1999:CCB

[KRS99] R. Kumar, S. Rajagopalan, and A. Sahai. Coding constructions for blacklisting problems without computational assumptions. In Wiener [Wie99], pages 609–623. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Kruh:1998:WWS

[Kru98] Louis Kruh. Why was Safford pessimistic about breaking the German Enigma cipher machine in 1942? In Deavours et al. [DKK+98], pages 235–239. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Knudsen:1999:TDS

[KRW99] L. R. Knudsen, M. J. B. Robshaw, and D. Wagner. Truncated differentials and Skipjack. In Wiener [Wie99], pages 165–180. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Kordes:1989:UMC

[KS89] F. L. G. Kordes and J. J. Schuurman. The use of MEBAS in creating a simulation environment for compression and encryption. Report NLR TP 89130 U, National Lucht-en Ruimtevaartlaboratorium, Amsterdam, The Netherlands, 1989. 69 pp.

Kelsey:1997:CPO

[KS97a] J. Kelsey and B. Schneier. Conditional purchase orders. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, April 1997. URL `http://www.counterpane.com/conditional_purchase_orders.html`. Also published in *4th ACM Conference on Computer and Communications Security*, ACM Press, April 1997, pp. 117–124.

Kurosawa:1997:DSP

[KS97b] Kaoru Kurosawa and Takashi Satoh. Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria. *Lecture Notes in Computer Science*, 1233:434–449, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330434.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1233/12330434.pdf`.

Kwon:1997:SEA

[KS97c] T. Kwon and J. Song. Security and efficiency in authentication protocols resistant to password guessing attacks. In IEEE Computer Society. Technical Committee on Computer Communications [IEE97l], pages 245–252. ISBN 0-8186-8141-1, 0-8186-8142-X (casebound), 0-8186-8143-8 (microfiche). ISSN 0742-1303. LCCN TK5105.5 .C82 1997. IEEE Computer Society Press order number PR08141. IEEE Order Plan number 97TB100179.

Kaliski:1998:RPRb

[KS98a] B. Kaliski and J. Staddon. RFC 2437: PKCS #1: RSA cryptography specifications version 2.0, October 1998. URL `ftp://ftp.internic.net/rfc/rfc2313.txt`; `ftp://ftp.internic.net/rfc/rfc2437.txt`; `https:/`

/www.math.utah.edu/pub/rfc/rfc2313.txt; https://www.math.utah.edu/pub/rfc/rfc2437.txt. Obsoletes RFC2313 [Kal98b]. Status: INFORMATIONAL.

Kelsey:1998:SPP

[KS98b] J. Kelsey and B. Schneier. The street performer protocol. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, November 1998. URL http://www.counterpane.com/street_performer.html. Also published in *The Third USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1998.

Kinoshita:1998:GST

[KS98c] H. Kinoshita and M. Satoh. Generation of the signature with the structured information of the image. In Theodoridis et al. [T+98], pages 2273–2276. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073141.html. Four volumes.

Kipnis:1998:COV

[KS98d] Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil and vinegar signature scheme. *Lecture Notes in Computer Science*, 1462: 257–266, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kelsey:1999:AST

[KS99a] John Kelsey and Bruce Schneier. Authenticating secure tokens using slow memory access. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1999. URL http://www.counterpane.com/slow-memory.html. First USENIX Symposium on Smart Cards, USENIX Press, to appear.

Kipnis:1999:CHP

[KS99b] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. *Lecture Notes in Computer Science*, 1666: 19–30, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660019.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660019.pdf.

Kemp:1996:CPC

[KSB96a] A. H. Kemp, S. J. Shepherd, and S. K. Barton. Correlation properties of a class of cryptographically secure spreading sequences. In *ISSSTA '96, 22–25 September 1996, Mainz, Germany*, page ?? ????, ????, 1996. ISBN ???? LCCN ????

Kemp:1996:PRM

[KSB96b] A. H. Kemp, S. J. Shepherd, and S. K. Barton. Progress report on multifunction coding and modulation for spread spectrum and CDMA with inherent security. In ????, editor, *EPSRC Annual Conference on Communications, Signal Processing and Coding, 30–31 January 1996, Sheffield, UK*, page ?? ????, ????, 1996. ISBN ???? LCCN ????

Kemp:1997:MFC

[KSB97] A. H. Kemp, S. J. Shepherd, and S. K. Barton. Multifunction coding and modulation for spread spectrum and CDMA with inherent security. In ????, editor, *EPSRC Annual Conference on Communications, Signal Processing and Coding, 22–23 January 1997, Sheffield, UK*, page ?? ????, ????, 1997. ISBN ???? LCCN ????

Kelsey:1999:NDA

[KSF99] J. Kelsey, B. Schneier, and N. Ferguson. Notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator. In *Sixth Annual Workshop on Selected Areas in Cryptography*, page ???? Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN ???? LCCN ???? URL `http://www.counterpane.com/yarrow-notes.html`.

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.

Kelsey:1997:SAL

[KSHW97] J. Kelsey, B. Schneier, C. Hall, and D. Wagner. Secure applications of low-entropy keys. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, September 1997. URL `http://www.counterpane.com/low-entropy.html`. Also published in *1997 Information Security Workshop (ISW'97)*, September 1997, pp. 121–134 [KSHW98].

Kelsey:1998:SAL

[KSHW98] J. Kelsey, B. Schneier, C. Hall, and D. Wagner. Secure applications of low-entropy keys. *Lecture Notes in Computer Science*, 1396: 121–134, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/low-entropy.html`. See [KSHW97].

Kim:1996:EIE

[KSK96] Yong-Tae Kim, Kwang-Suk Suh, and Chang-Han Kim. On the efficient implementations of the elliptic curve ElGamal cryptosystem. *Bull. Honam Math. Soc.*, 13:249–256, 1996. ISSN 1225-2921.

Kehne:1992:NBP

[KSL92] A. Kehne, J. Schönwälder, and H. Langendörfer. A nonce-based protocol for multiple authentications. *Operating Systems Review*, 26(4):84–89, October 1992. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Knowles:1992:AFC

[KSS+92] Brad Knowles, Roger Schlafly, Grant D. Schultz, Lynn Zelvin, Paul Heckel, and E. Robert Yoches. ACM Forum: Comments on cryptography. *Communications of the Association for Computing Machinery*, 35(11): 19–24, 112, November 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Kelsey:1996:KCI

[KSW96] John Kelsey, Bruce Schneier, and David Wagner. Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. *Lecture Notes in Computer Science*, 1109:237–251, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/key_schedule.html`.

Kelsey:1997:RCB

[KSW97a] J. Kelsey, B. Schneier, and D. Wagner. Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X NewDES, RC2, and TEA. *Lecture Notes in Computer Science*, 1334: 233–246, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/related-key_cryptanalysis.html`.

Kelsey:1997:RKC

[KSW97b] J. Kelsey, B. Schneier, and D. Wagner. Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X NewDES, RC2, and TEA. *Lecture Notes in Computer Science*, 1334: 233–246, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/related-key_cryptanalysis.html`.

Kelsey:1998:PICa

[KSW98a] J. Kelsey, B. Schneier, and D. Wagner. Protocol interactions and the chosen protocol attack. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. URL `http://www.counterpane.com/chosen_protocol.html`. Also published in *Security Protocols, 5th International Workshop April 1997 Proceedings*, Springer-Verlag, 1998, pp. 91–104.

Kelsey:1998:PICb

[KSW98b] J. Kelsey, B. Schneier, and D. Wagner. Protocol interactions and the chosen protocol attack. *Lecture Notes in Computer Science*, 1361:91–104, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/chosen_protocol.html`.

Kelsey:1999:KSWa

[KSW99a] J. Kelsey, B. Schneier, and D. Wagner. Key schedule weakness in SAFER+. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1999. URL `http://www.counterpane.com/safer.html`. Second AES Candidate Conference, April 1999, to appear.

Kelsey:1999:MCAa

[KSW99b] J. Kelsey, B. Schneier, and D. Wagner. Mod n cryptanalysis, with applications against RC5P and M6. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1999. URL `http://www.counterpane.com/mod3.html`. Fast Software Encryption, Sixth International Workshop Proceedings (March 1999), Springer-Verlag, 1999, to appear.

Kelsey:1999:MCAb

[KSW99c] J. Kelsey, B. Schneier, and D. Wagner. Mod n cryptanalysis, with applications against RC5P and M6. In Knudsen [Knu99c], pages 139–155. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1636/16360139.htm; http://link.springer-ny.com/link/service/series/0558/papers/1636/16360139.pdf`.

Kelsey:1998:SCCa

[KSWH98a] J. Kelsey, B. Schneier, D. Wagner, and C. Hall. Side channel cryptanalysis of product ciphers. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. URL `http://www.counterpane.com/side_channel.html`. Also published in ESORICS '98 Proceedings, Springer-Verlag, September 1998, pp. 97–110.

Kelsey:1998:SCCb

[KSWH98b] J. Kelsey, B. Schneier, D. Wagner, and C. Hall.

Side channel cryptanalysis of product ciphers. In Quisquater et al. [Q+98], page ?? ISBN 3-540-65004-0. LCCN QA267.A1 L43 no.1485.

Kelsey:1998:SCCc

[KSWH98c] J. Kelsey, B. Schneier, D. Wagner, and C. Hall. Side channel cryptanalysis of product ciphers. *Lecture Notes in Computer Science*, 1485:97–110, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/side_channel.html`.

Kelsey:1998:CAP

[KSWH98d] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic attacks on pseudorandom number generators. *Lecture Notes in Computer Science*, 1372:168–188, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/pseudorandom_number.html`; `http://www.schneier.com/paper-prngs.html`.

Korzhik:1991:CMP

[KT91a] Valery I. Korzhik and Andrey I. Turkin. Cryptanalysis of McEliece's public-key cryptosystem. *Lecture Notes in Computer Science*, 547:68–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470068.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0547/05470068.pdf`.

Koyama:1991:NPC

[KT91b] K. Koyama and R. Terada. Nonlinear parity circuits and their cryptographic applications. *Lecture Notes in Computer Science*, 537:582–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Koyama:1993:SEC

[KT93] Kenji Koyama and Yukio Tsuruoka. Speeding up elliptic cryptosystems by using a signed binary window method. *Lecture Notes in Computer Science*, 740:345–357, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Keefe:1996:MTS

[KT96] T. F. Keefe and W. T. Tsai. A multiversion transaction scheduler for centralized multilevel secure database systems. In IEEE [IEE96d], pages 206–213. ISBN 0-8186-7629-9 (paperback), 0-8186-7631-0 (microfiche). LCCN

TA168.I199 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/063213.html. IEEE Computer Society Press Order Number PR07629. IEEE Order Plan Catalog Number 96TB100076.

Koyama:1998:AFC

[KT98] K. Koyama and R. Terada. An augmented family of cryptographic parity circuits. *Lecture Notes in Computer Science*, 1396: 198–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kim:1999:AFC

[KT99] Eugene Eric Kim and Betty Alexandra Toole. Ada and the first computer: The collaboration between Ada, Countess of Lovelace, and computer pioneer Charles Babbage resulted in a landmark publication that described how to program the world's first computer. *Scientific American*, 280(5):76–81, May 1999. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). See also [AAG+00].

Kanda:1999:SCF

[KTM+99] Masayuki Kanda, Youichi Takashima, Tsutomu Matsumoto, Kazumaro Aoki, and Kazuo Ohta. A strategy for constructing fast round functions with practical security against differential and linear cryptanalysis. *Lecture Notes in Computer Science*, 1556: 264–279, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kuchlin:1987:PKE

[Küc87] W. Küchlin. Public key encryption. *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 21 (3):69–73, August 1987. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

Kucera:1992:GES

[Kuč92] Luděk Kučera. A generalized encryption scheme based on random graphs. In *Graph-theoretic concepts in computer science (Fischbachau, 1991)*, volume 570 of *Lecture Notes in Comput. Sci.*, pages 180–186. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992.

Kuhn:1998:CIS

[Kuh98] M. G. Kuhn. Cipher instruction search attack on the bus-encryption security microcontroller DS5002FP. *IEEE Transactions on Computers*, 47(10):1153–1157, October 1998. CO-

DEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=729797.

Kuijk:1991:RSE

[Kui91] A. A. M. Kuijk. Report on the Sixth Eurographics Workshop on Graphics Hardware. *Computer Graphics Forum*, 10(4):363–364, December 1991. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Kukorelly:1999:VCH

[Kuk99] Zsolt Kukorelly. *On the validity of certain hypotheses used in linear cryptanalysis*. Thesis (Ph.D.), Technische Hoschule, Zürich, Zürich, Switzerland, 1999. English text with German abstract. Published by Hartung-Gorre, Konstanz, Switzerland.

Kullback:1935:SMC

[Kul35] Solomon Kullback. *Statistical methods in cryptanalysis: technical paper*. War Dept., Office of the Chief Signal Officer: U.S. G.P.O., Washington, DC, USA, 1935. various pp.

Kullback:1938:SMC

[Kul38] Solomon Kullback. *Statistical methods in cryptanalysis*. War Department, Office of the Chief Signal Officer, Washington, DC, USA, revised edition, 1938. 194 pp.

Kullback:1967:SMC

[Kul67] Solomon Kullback. *Statistical methods in cryptanalysis*. Number 14 in Technical literature series monograph. National Archives, Washington, DC, USA, revised edition, 1967. iii + 194 pp.

Kullback:1976:SMC

[Kul76] Solomon Kullback. *Statistical methods in cryptanalysis*, volume 4 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, revised edition, 1976. v + 206 pp. LCCN Z104 .K84.

Kumar:1997:CSI

[Kum97] I. J. Kumar. *Cryptology: system identification and key-clustering*, volume 78 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1997. ISBN 0-89412-267-3. vii + 492 pp. LCCN ????

Kummert:1998:RPT

[Kum98] H. Kummert. RFC 2420: The PPP triple-DES encryption protocol (3DESE), September 1998. URL ftp://ftp.internic.net/rfc/rfc2420.txt; https://www.math.utah.edu/pub/rfc/rfc2420.txt. Status: PROPOSED STANDARD.

Kuo:1990:TEC

[Kuo90] Chung Jung Kuo. *Transform encryption coding.* Thesis (Ph.D.), Department of Electrical Engineering, Michigan State University, East Lansing, MI 48824, USA, 1990. vi + 101 pp.

Kurosawa:1994:NBA

[Kur94] Kaoru Kurosawa. New bound on authentication code with arbitration. In Desmedt [Des94b], pages 140–149. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390140.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0839/08390140.pdf`.

Kearns:1989:CLL

[KV89] M. Kearns and L. G. Valiant. Cryptographic limitations on learning Boolean formulae and finite automata. In ACM-TOC'89 [ACM89c], pages 433–444. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. URL `http://www.acm.org/pubs/articles/proceedings/stoc/73007/p433-kearns/p433-kearns.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/73007/p433-kearns/`.

Kearns:1994:CLL

[KV94] Michael Kearns and Leslie Valiant. Cryptographic limitations on learning Boolean formulae and finite automata. *Journal of the Association for Computing Machinery*, 41(1):67–95, January 1994. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/174647.html`.

Kaul:1999:IBP

[KV99] M. Kaul and R. Vemuri. Integrated block-processing and design-space exploration in temporal partitioning for RTR architectures. *Lecture Notes in Computer Science*, 1586: 606–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kirstein:1992:PAS

[KW92] P. T. Kirstein and P. Williams. Piloting authentication and security services within OSI applications for RTD information (PASSWORD). *Computer Networks and ISDN Systems*, 25(4–5): 483–??, November 1992. CODEN CNISE9. ISSN

0169-7552 (print), 1879-2324 (electronic).

Konrad:1999:SDK

[KW99] K. Konrad and D. A. Wolfram. System description: Kimba, a model generator for many-valued first-order logics. *Lecture Notes in Computer Science*, 1632: 282–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kwan:1993:SAD

[Kwa93] Matthew Kwan. Simultaneous attacks in differential cryptanalysis (getting more pairs per encryption). *Lecture Notes in Computer Science*, 739:489–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kwan:1997:DIE

[Kwa97] Matthew Kwan. The design of the ICE encryption algorithm. *Lecture Notes in Computer Science*, 1267:69–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670069.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1267/12670069.pdf`.

Kaliski:1995:SRE

[KY95a] Burt Kaliski and Yiqun Lisa Yin. On the security of the RC5 encryption algorithm. *CryptoBytes*, 1(2): 13–14, Summer 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf`.

Kaliski:1995:DLC

[KY95b] Burton S. Kaliski Jr. and Yiqun Lisa Yin. On differential and linear cryptanalysis of the RC5 encryption algorithm. In Coppersmith [Cop95d], pages 171–183. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630171.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0963/09630171.pdf`. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Kaliski:1997:SRE

[KY97] B. S. Kaliski, Jr. and Y. L. Yin. On the security of the RC5 encryption algorithm. Technical report, RSA Data Security, Inc., Redwood City, CA, USA, 1997. In preparation.

Kaliski:1998:SRE

[KY98] Burton S. Kaliski, Jr. and Yiqun Lisa Yin. On the security of the RC5 encryption algorithm. Technical report TR-602, RSA Data Security, Inc., Redwood City, CA, USA, September 1998. 39 pp. URL ftp://ftp.rsasecurity.com/pub/rsalabs/rc5/rc5-report.pdf. Version 1.0.

Kaliski:19xx:DLC

[KYxx] B. S. Kaliski, Jr. and Y. L. Yin. On differential and linear cryptanalysis of the RC5 encryption algorithm. Accepted to Crypto '95., 19xx.

Kwok-Yan:1992:TAD

[KYB92] Lam Kwok-Yan and Thomas Beth. Timely authentication in distributed systems. *Lecture Notes in Computer Science*, 648: 293–??, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kurosawa:1998:SBC

[KYDB98] Kaoru Kurosawa, Takuya Yoshida, Yvo Desmedt, and Mike Burmester. Some bounds and a construction for secure broadcast encryption. *Lecture Notes in Computer Science*, 1514: 420–433, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kwok-Yan:1992:FAA

[KYG92] Lam Kwok-Yan and Dieter Gollmann. Freshness assurance of authentication protocols. *Lecture Notes in Computer Science*, 648: 261–??, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kasami:1982:KMS

[KYM82] Tadao Kasami, Saburo Yamamura, and Kenichi Mori. A key management scheme for end-to-end encryption and a formal verification of its security. *Systems-Comput.-Controls*, 13(3): 59–69 (1983), 1982. CODEN SYCCBB. ISSN 0096-8765.

Koch:1995:TRH

[KZ95] E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In Pitas [Pit95], pages 452–455. LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1005.html. Two volumes.

Levien:1998:ART

[LA98] Raph Levien and Alex Aiken. Attack-resistant trust metrics for public key certification. In USENIX

[USE98d], page ?? ISBN 1-880446-92-8. LCCN QA76.9.A25 U83 1998. URL http://www.usenix.org/publications/library/proceedings/sec98/levien.html.

Lampson:1991:ADS

[LABW91] Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: theory and practice. *Operating Systems Review*, 25(5):165–182, October 1991. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lampson:1992:ADS

[LABW92] Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310, November 1992. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic). URL http://www.acm.org:80/pubs/citations/journals/tocs/1992-10-4/p265-lampson/.

Lacy:1993:CCS

[Lac93] John B. Lacy. CryptoLib: Cryptography in software. In USENIX Association [USE93], pages 1–17. ISBN 1-880446-55-3. LCCN QA 76.9 A25 U54 1993.

Laffin:1964:CCS

[Laf64] John Laffin. *Codes and ciphers: secret writing through the ages*. Abelard-Schuman, ????, 1964. 164 pp.

Lagarias:1984:KPK

[Lag84a] J. C. Lagarias. Knapsack public key cryptosystems and Diophantine approximation (extended abstract). In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 3–23. Plenum, New York, 1984.

Lagarias:1984:PAS

[Lag84b] J. C. Lagarias. Performance analysis of Shamir's attack on the basic Merkle–Hellman knapsack cryptosystem. *Lecture Notes in Computer Science*, 172: 312–323, 1984. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lagarias:1990:PNG

[Lag90] J. C. Lagarias. Pseudorandom number generators in cryptography and number theory. In Pomerance and Goldwasser [PG90], pages 115–143. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990.

Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

Lai:1992:DSB

[Lai92] Xuejia Lai. *On the design and security of block ciphers*. Hartung-Gorre Verlag, Konstanz, Switzerland, 1992. ISBN 3-89191-573-X. xii + 108 pp. LCCN QA76.9.A25L335 1992. This is the author's Ph.D. dissertation. "Secret-key block ciphers are the subject of this work. The design and security of block ciphers, together with their application in hashing techniques, are considered. In particular, iterated block ciphers that are based on iterating a weak round function several times are considered. Four basic constructions for the round function of an iterated cipher are studied.".

Lai:1995:ALS

[Lai95] X. Lai. Additive and linear structures of cryptographic functions. *Lecture Notes in Computer Science*, 1008:75–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lakshmivarahan:1983:APK

[Lak83] S. Lakshmivarahan. Algorithms for public key cryptosystems: theory and application. In *Advances in computers, Vol. 22*, volume 22 of *Adv. in Comput.*, pages 45–108. Academic Press, New York, NY, USA, 1983.

Lampson:1973:NCP

[Lam73] Butler W. Lampson. A note on the confinement problem. *Communications of the Association for Computing Machinery*, 16(10):613–615, October 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1014.html`.

Lamport:1981:TNP

[Lam81] Leslie Lamport. Technical note: Password authentication with insecure communication. *Communications of the Association for Computing Machinery*, 24(11):770–772, November 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Lambert:1999:DSV

[Lam99] James D. Lambert. DREO secure video conferencing and high speed data encryption tests for Inmarsat-

B satellite terminals. Technical memorandum DREO TM 1999-084, Defence Research Establishment Ottawa, Ottawa, ON, Canada, 1999. xiii + 17 + 21 pp.

Landers:1946:RPR

[Lan46] A. W. Landers. Recent publications: Reviews: *An Historical and Analytical Bibliography of the Literature of Cryptology*, by J. S. Galland. *American Mathematical Monthly*, 53(6):330–331, June/July 1946. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Langie:1981:CSS

[Lan81] Andre Langie. *Cryptography: a study on secret writings*, volume 38 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1981. ISBN 0-89412-061-1. vii + 192 pp. LCCN Z104 .L28 1981. Translation of: De la cryptographie. Reprint of an unspecified previous ed. Bibliography: p. 158.

Landau:1989:SSC

[Lan89] Charles R. Landau. Security in a secure capability-based system. *Operating Systems Review*, 23(4):2–4, October 1989. CODEN OSRED8. ISSN 0163-5980.

Langford:1995:DCT

[Lan95] Susan K. Langford. *Differential-linear cryptanalysis and threshold signatures*. Thesis (Ph.D.), Department of Electrical Engineering, Stanford University, Stanford, CA, USA, 1995. xi + 98 pp.

Langford:1996:WST

[Lan96] Susan K. Langford. Weaknesses in some threshold cryptosystems. *Lecture Notes in Computer Science*, 1109:74–82, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lange:1997:SCI

[Lan97] N. Lange. Single-chip implementation of a cryptosystem for financial applications. *Lecture Notes in Computer Science*, 1318: 135–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Landrock:1998:TOC

[Lan98] P. Landrock. TTPs overview — concepts and review of the state of the art from a technical point of view. *Lecture Notes in Computer Science*, 1528: 241–263, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Landrock:1999:PTU

[Lan99] Peter Landrock. Primality tests and use of primes in public key systems. *Lecture Notes in Computer Science*, 1561:127–133, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1561/15610127.htm; http://link.springer-ny.com/link/service/series/0558/papers/1561/15610127.pdf.

Lassek:1985:CCA

[Las85] Teresa A. Lassek. Cryptology and the computer age. Thesis (Honors), University of Nebraska at Omaha, Omaha, NE, USA, 1985. 58 pp.

Lassak:1992:SRP

[Laš92] Miroslav Laššák. Some remarks on the Pethő public key cryptosystem. *Astérisque*, 209:15, 257–264, 1992. ISSN 0303-1179. Journées Arithmétiques, 1991 (Geneva).

Lauer:1981:CSC

[Lau81] Rudolph F. Lauer. *Computer simulation of classical substitution cryptographic systems*, volume 32 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1981. ISBN 0-89412-050-6. xi + 111 pp. LCCN Z104 .L38 1981.

Lawton:1998:NBS

[Law98] George Lawton. News briefs: Sun joins tetherless network fray; private doorbells: Solution to encryption controversy; Web extensions promise distributed computing; Wall Street conducts major Y2K test; Sun prepares to submit first Java standard; Netscape loses more ground in browser war. *Computer*, 31(10):17–19, October 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co1998/pdf/rx017.pdf.

Lee:1988:OSM

[LB88] P. J. Lee and E. F. Brickell. An observation on the security of McEliece's public-key cryptosystem. *Lecture Notes in Computer Science*, 330:275–280, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lee:1989:WBL

[LB89a] T. Paul Lee and R. E. Barkley. A watermark-based lazy buddy system for kernel memory allocation. In USENIX [USE89a], pages 1–13.

Lee:1989:WLB

[LB89b] T. Paul Lee and R. E. Barkley. A watermark-based lazy buddy system for kernel memory allocation. In USENIX Association [USE89b], pages 1–13. LCCN QA 76.76 O63 U83 1989.

Leake:1999:IIR

[LBHM99] D. B. Leake, L. Birnbaum, K. Hammond, and C. Marlow. Integrating information resources: a case study of engineering design support. *Lecture Notes in Computer Science*, 1650:482–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Landwehr:1994:TCP

[LBMC94] Carl E. Landwehr, Alan R. Bull, John P. McDermott, and William S. Choi. A taxonomy of computer program security flaws. *ACM Computing Surveys*, 26(3):211–254, September 1994. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0360-0300/185412.html`.

Low:1994:SAP

[LC94] M. R. Low and B. Christianson. Self authenticating proxies. *The Computer Journal*, 37(5):422–428, ???? 1994. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Lomas:1995:RBH

[LC95] Mark Lomas and Bruce Christianson. Remote booting in a hostile world: to whom am I speaking? (computer security). *Computer*, 28(1):50–54, January 1995. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Lee:1996:IAP

[LC96a] Wei-Bin Lee and Chin-Chen Chang. Integrating authentication in public key distribution system. *Information Processing Letters*, 57(1): 49–52, January 15, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lin:1996:BCC

[LC96b] J.-F. Lin and S.-J. Chen. Broadcasting cryptosystem in computer networks using interpolating polynomials. *International Journal of Computer Systems Science and Engineering*, 11 (5):315–??, ???? 1996. CODEN CSSEEI. ISSN 0267-6192.

Lin:1996:CBC

[LC96c] Jiann-Fu Lin and Sao-Jie Chen. Comment on 'Broadcasting cryptosystem in computer networks using interpolating polynomials'. *International Journal of Computer Systems Science and Engineering*, 11(5):315–317, September 1996. CODEN CSSEEI. ISSN 0267-6192.

Lee:1997:AES

[LC97a] Wei-Bin Lee and Chin-Chen Chang. Authenticated encryption schemes with linkage between message blocks. *Information Processing Letters*, 63(5):247–250, September 24, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lou:1997:PTL

[LC97b] Der-Chyuan Lou and Chin-Chen Chang. A parallel two-list algorithm for the knapsack problem. *Parallel Computing*, 22(14):1985–1996, March 1997. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Lou:1998:FMM

[LC98] Der-Chyuan Lou and Chin-Chen Chang. A fast modular multiplication method. *International Journal of Computer Systems Science and Engineering*, 13(6): 353–358, November 1998. CODEN CSSEEI. ISSN 0267-6192.

Lacan:1999:SOE

[LC99] J. Lacan and P. Chatonnay. Search of optimal error correcting codes with genetic algorithms. *Lecture Notes in Computer Science*, 1625:93–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lin:1992:RCD

[LCL92] C. H. Lin, C. C. Chang, and R. C. T. Lee. A record-oriented cryptosystem for database sharing. *The Computer Journal*, 35(6): 658–660, December 1992. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Lin:1995:NPK

[LCL95] C. H. Lin, C. C. Chang, and R. C. T. Lee. A new public-key cipher system based upon the Diophantine equations. *IEEE Transactions on Computers*, 44 (1):13–19, January 1995. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=368013`. See comment [BMP97a].

Leung:1999:DIM

[LCN99] C.-H. Leung, K.-M. Cheung, and T.-F. Ngai. Design and implementation of a mobile application support system. *Lecture Notes in Computer Science*, 1552: 347–357, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lopez:1999:IAE

[LD99] J. Lopez and R. Dahab. Improved algorithms for elliptic curve arithmetic in GF(2n0n). *Lecture Notes in Computer Science*, 1556: 201–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Li:1994:EMN

[LDW94] Yuan Xing Li, Robert H. Deng, and Xin Mei Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40 (1):271–273, 1994. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Lin:1999:AMG

[LE99] X. Lin and P. Eades. Area minimization for grid visibility representation of hierachically planar graphs. *Lecture Notes in Computer Science*, 1627:92–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Leary:1987:CSM

[Lea87] Penn Leary. *The Cryptographic Shakespeare: a monograph wherein the poems and plays attributed to William Shakespeare are proven to contain the enciphered name of the concealed author, Francis Bacon.* Westchester House, Omaha, NE, USA, 1987. ISBN 0-9617917-0-5. 272 pp. LCCN PR2944 .L38 1987.

Leary:1990:SCS

[Lea90] Penn Leary. *The second cryptographic Shakespeare: a monograph wherein the poems and plays attributed to William Shakespeare are proven to contain the enciphered name of the concealed author, Francis Bacon.* Westchester House, Omaha, NE, USA, enlarged edition, 1990. ISBN 0-9617917-1-3. 313 pp. LCCN PR2944 .L38 1990.

Lear:1999:NBE

[Lea99] Anne C. Lear. News briefs: Explorer worm targets networks; H-1B visa cap reached; higher limit proposed; encryption industry grows outside US; software design flaw spurs lawsuits. *Computer*, 32(8): 15–17, August 1999. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http:`

//dlib.computer.org/co/books/co1999/pdf/r8015.pdf.

Leclerc:1989:CRM

[Lec89] Matthias Leclerc. Chinesische Reste und moderne Kryptographie. (German) [Chinese remainders and modern cryptography]. *Mathematische Semesterberichte*, 36(2):257–267, 1989. CODEN ???? ISSN 0720-728X.

Lee:1995:NSI

[Lee95] Hsun-Ming Lee. Network security integration by public key encryption and stored procedures of database servers. Thesis (M.S.E.), Arizona State University, Tempe, AZ, USA, 1995. ix + 90 pp.

Leech:1996:RUP

[Lee96] M. Leech. RFC 1929: Username/password authentication for SOCKS V5, April 1996. URL ftp://ftp.internic.net/rfc/rfc1929.txt; https://www.math.utah.edu/pub/rfc/rfc1929.txt. Status: PROPOSED STANDARD.

Lee:1999:GIC

[Lee99a] Annabelle Lee. *Guideline for implementing cryptography in the Federal Government*. Washington, DC, USA, November 1999. v + 133 pp. Shipping list no. 2000-0510-M.

Lee:1999:DAA

[Lee99b] J. Lee. Desiderata in agent architectures for coordinating multi-agent systems. *Lecture Notes in Computer Science*, 1599:47–60, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Leighton:1969:SCA

[Lei69] Albert C. Leighton. Secret communication among the Greeks and Romans. *Technology and Culture*, 10(2): 139–154, April 1969. CODEN TECUA3. ISSN 0040-165X (print), 1097-3729 (electronic). URL https://muse.jhu.edu/pub/1/article/892350/pdf.

Leighton:1979:BRA

[Lei79a] Albert C. Leighton. Book review: *An annotated bibliography of cryptography*: By David Shulman. Garland Reference Library of the Humanities, Vol. 37 New York/London (Garland Publishing Inc.). 1976. xvi + 372 pp. illus. $35.00. *Historia Mathematica*, 6(2): 213–218, May 1979. CODEN HIMADS. ISSN 0315-0860 (print), 1090-249X (electronic). URL http://www.sciencedirect.com/science/article/pii/0315086079900934.

Leighton:1979:BRB

[Lei79b] Albert C. Leighton. Book review: *An annotated bib-*

liography of cryptography: By David Shulman. Garland Reference Library of the Humanities, Vol. 37 New York/London (Garland Publishing Inc.). 1976. xvi + 372 pp. illus. $35.00. *Historia Mathematica*, 6(2): 213–218, May 1979. CODEN HIMADS. ISSN 0315-0860 (print), 1090-249X (electronic). URL http://www.sciencedirect.com/science/article/pii/0315086079900934.

Leiss:1980:NSS

[Lei80] E. Leiss. A note on a signature system based on probabilistic logic. *Information Processing Letters*, 11(2): 110–113, October ??, 1980. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Leipold:1999:K

[Lei99a] Cosimo Leipold. Kerberos. *Linux Journal*, 68:??, December 1999. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://noframes.linuxjournal.com/lj-issues/issue68/3329.html.

Leiserson:1999:ITD

[Lei99b] C. E. Leiserson. Invited talk: Design and analysis of algorithms for shared-memory multiprocessors. *Lecture Notes in Computer Science*, 1663:55–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lempel:1979:CT

[Lem79] Abraham Lempel. Cryptology in transition. *ACM Computing Surveys*, 11(4): 285–303, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Lennon:1978:CAI

[Len78] Richard E. Lennon. Cryptography architecture for information security. *IBM Systems Journal*, 17(2): 138–150, 1978. CODEN IBMSA7. ISSN 0018-8670.

Lenstra:1987:FIE

[Len87] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987. CODEN ANMAAH. ISSN 0003-486X (print), 1939-8980 (electronic). URL http://www.jstor.org/stable/1971363.

Lenstra:1990:PT

[Len90] Arjen K. Lenstra. Primality testing. In Pomerance and Goldwasser [PG90], pages 13–25. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

Lennox:1993:ES

[Len93] G. Lennox. EDI security. *Lecture Notes in Computer Science*, 741:235–243, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lenstra:1996:GSD

[Len96a] A. K. Lenstra. Generating standard DSA signatures without long inversion. *Lecture Notes in Computer Science*, 1163:57–64, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lenstra:1996:VNS

[Len96b] A. K. Lenstra. Viewpoint: Network security — elusive, essential. *IEEE Spectrum*, 33(1):32–33, January 1996. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Lenstra:1998:GRM

[Len98] A. K. Lenstra. Generating RSA moduli with a predetermined portion. *Lecture Notes in Computer Science*, 1514:1–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lenstra:1999:EIB

[Len99a] A. K. Lenstra. Efficient identity based parameter selection for elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 1587:294–302, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lenzerini:1999:DLT

[Len99b] M. Lenzerini. Description logics and their relationships with databases. *Lecture Notes in Computer Science*, 1540:32–38, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lercier:1997:FGR

[Ler97] Reynald Lercier. Finding good random elliptic curves for cryptosystems defined over $\mathbf{F}_{2^n}$. *Lecture Notes in Computer Science*, 1233:379–392, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Levine:1958:VMS

[Lev58] Jack Levine. Variable matrix substitution in algebraic cryptography. *American Mathematical Monthly*, 65(3):170–179, March 1958. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Levine:1961:SAH

[Lev61a] Jack Levine. Some applications of high-speed computers to the case $n = 2$ of algebraic cryptography. *Mathematics of Computation*, 15 (75):254–260, July 1961. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Levine:1961:SECa

[Lev61b] Jack Levine. Some elementary cryptanalysis of algebraic cryptography. *American Mathematical Monthly*, 68(5):411–418, May 1961. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Levine:1961:SECb

[Lev61c] Jack Levine. *Some elementary cryptanalysis of algebraic cryptography*. Mathematical Association of America, Buffalo, NY, USA, 1961. 411–418 pp. Reprint from American Mathematical Monthly, vol. 68, no. 5, May 1961.

Levine:1983:USC

[Lev83] Jack Levine. *United States cryptographic patents, 1861–1981*. Cryptologia, Terre Haute, IN, USA, 1983. ISBN 0-9610560-0-2. 69 pp. LCCN T223.Z1 .L48.

Levin:1985:OWF

[Lev85] L. A. Levin. One-way functions and pseudorandom generators. In ACM [ACM85], pages 363–365. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6 A13 1985. URL `http://www.acm.org/pubs/articles/proceedings/stoc/22145/p363-levin/p363-levin.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/22145/p363-levin/`. ACM order no. 508850.

Levine:1991:USC

[Lev91] Jack Levine. *United States cryptographic patents, 1861–1989*. Cryptologia, Terre Haute, IN, USA, second edition, 1991. ISBN 0-9610560-1-0. 115 pp. LCCN Z103 .L66 1991.

Lewin:1978:UGW

[Lew78] Ronald Lewin. *Ultra goes to war: the first account of World War II's greatest secret based on official documents*. McGraw-Hill, New York, NY, USA, 1978. ISBN 0-07-037453-8. 397 + 6 pp. LCCN D810.S7 L43 1978; D810.S7L43. US$12.95.

Lewin:1982:AMC

[Lew82] Ronald Lewin. *The American magic: codes, ciphers, and the defeat of Japan*. Farrar Straus Giroux, New York, NY, USA, 1982. ISBN 0-374-10417-4. xv + 332 pp. LCCN D810.C88 .L48.

Lewis:1992:SCP

[Lew92] Frank W. Lewis. *Solving cipher problems: cryptanalysis, probabilities and diagnostics*, volume 58 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1992. ISBN 0-89412-179-0, 0-89412-178-2. v + 253 + 12 pp. LCCN ????

Lexar:1976:END

[Lex76] Lexar Corporation. An evaluation of the NBS Data Encryption Standard. Unpublished report, Lexar Corporation, 11611 San Vicente Boulevard, Los Angeles, CA, USA, 1976.

Laurin:1997:SSM

[LF97] Fredrik Laurin and Calle Froste. Secret Swedish e-mail can be read by the U.S.A. Web site, November 1997. URL `http://catless.ncl.ac.uk/Risks/19.52.html`.

Lopes:1999:UES

[LF99] A. Lopes and J. L. Fiadeiro. Using explicit state to describe architectures. *Lecture Notes in Computer Science*, 1577:144–160, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lorigo:1999:CDG

[LFCK99] L. M. Lorigo, O. Faugeras, W. E. L. Crimson, and R. Keriven. Co-dimension 2 geodesic active contours for MRA segmentation. *Lecture Notes in Computer Science*, 1613:126–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Li:1994:RMC

[LFSY94] X. A. Li, J. H. Fu, Y. G. Song, and H. Y. Yang. Recursive mappings for computer virus. In Xiao et al. [XtTmW94], pages 279–286. ISBN 7-03-004363-4. LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/034404.html`.

Laih:1997:CDE

[LG97] C. S. Laih and M. J. Gau. Cryptanalysis of a Diophantine equation oriented public key cryptosystem. *IEEE Transactions on Computers*, 46 (4):511–512, April 1997. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=588074`.

Laih:1993:GTC

[LH93a] Chi-Sung Laih and Lein Harn. Generalized threshold cryptosystems. *Lecture Notes in Computer Science*, 739:159–??, 1993. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Lin:1993:GSS

[LH93b] Hung-Yu Lin and Lein Harn. A generalized secret sharing scheme with cheater detection. *Lecture Notes in Computer Science*, 739:149–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Langford:1994:DLC

[LH94] Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. In Desmedt [Des94b], pages 17–25. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390017.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390017.pdf.

Lin:1995:FRS

[LH95] Hung-Yu Lin and Lein Harn. Fair reconstruction of a secret. *Information Processing Letters*, 55(1):45–47, July 7, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lichota:1996:VCP

[LHB96] Randall W. Lichota, Grace L. Hammonds, and Stephen H. Brackin. Verifying cryptographic protocols for electronic commerce. In USENIX [USE96b], pages 53–65.

Li:1994:RTR

[LHL94] Chuan-Ming Li, Tzonelih Hwang, and Narn-Yih Lee. Remark on the threshold RSA signature scheme. *Lecture Notes in Computer Science*, 773:413–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730413.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730413.pdf.

Li:1995:TSW

[LHL95a] C.-M. Li, T. Hwang, and N.-Y. Lee. Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders. *Lecture Notes in Computer Science*, 950:194–204, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Li:1995:TMS

[LHL95b] Chuan-Ming Li, Tzonelih Hwang, and Narn-Yih Lee.

Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders. *Lecture Notes in Computer Science*, 950: 194–204, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500194.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0950/09500194.pdf`.

Landwehr:1984:SMM

[LHM84] Carl E. Landwehr, Constance L. Heitmeyer, and John McLean. A security model for military message system. *ACM Transactions on Computer Systems*, 2 (3):198–222, August 1984. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Lee:1998:ZNP

[LHW98] N.-Y. Lee, T. Hwang, and C.-H Wang. On Zhang's nonrepudiable proxy signature schemes. *Lecture Notes in Computer Science*, 1438:415–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lee:1999:STI

[LHW99] Narn-Yih Lee, Tzonelih Hwang, and Chih-Hung Wang. The security of two ID-based multisignature protocols for sequential and broadcasting architectures. *Information Processing Letters*, 70(2):79–81, April 30, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lichtenthal:1994:CBT

[Lic94] Sigfrido Lichtenthal. Connect business and technology. *Datamation*, 40(22): 61–62, 64, November 15, 1994. CODEN DTMNAT. ISSN 0011-6963.

Lidl:1985:CBP

[Lid85] R. Lidl. On cryptosystems based on polynomials and finite fields. *Lecture Notes in Computer Science*, 209:10–15, 1985. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lidl:1990:SMA

[Lid90] Rudolf Lidl. Some mathematical aspects of recent advances in cryptology. In Loxton [Lox90], pages 1–8. ISBN 0-521-39877-0. LCCN Z103 .N845 1990. Papers presented at the 33rd Annual Meeting of the Australian Mathematical Society and at a Workshop on Number Theory and Cryptography in Telecommunications held at Macquarie

University in Sydney from 29 June to 7 July 1989.

Lieberherr:1981:UCD

[Lie81] K. Lieberherr. Uniform complexity and digital signatures. *Theoretical Computer Science*, 16(1):99–110, October 1981. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Liebl:1993:ADS

[Lie93] Armin Liebl. Authentication in distributed systems: a bibliography. *Operating Systems Review*, 27(4):31–41, October 1993. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lim:1998:CNB

[Lim98] Chae Hoon Lim. CRYPTON: a new 128-bit block cipher. In National Institute of Standards and Technology [Nat98], page 38. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf1/crypton-slides.ps`. Only the slides for the conference talk are available.

Lim:1999:RVC

[Lim99] C. H. Lim. A revised version of CRYPTON: CRYPTON V1.0. In Knudsen [Knu99c], pages 31–45. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

RFC0989

[Lin87] J. Linn. RFC 989: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures, February 1, 1987. URL `ftp://ftp.internic.net/rfc/rfc1040.txt`; `ftp://ftp.internic.net/rfc/rfc1113.txt`; `ftp://ftp.internic.net/rfc/rfc989.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1040.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1113.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc989.txt`. Obsoleted by RFC1040, RFC1113 [Lin88b, Lin89b]. Status: UNKNOWN.

Linn:1988:RPE

[Lin88a] J. Linn. RFC 1040: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures, January 1, 1988. URL `ftp://ftp.internic.net/rfc/rfc1040.txt`; `ftp://ftp.internic.net/rfc/rfc1113.txt`; `ftp://ftp.internic.net/rfc/rfc989.txt`; `https://www.math.utah.edu/pub/rfc/rfc1040.txt`; `https://www.math.utah.edu/pub/rfc/rfc1113.txt`; `https://www.math.utah.edu/pub/rfc/rfc989.txt`. Obsoleted by RFC1113 [Lin89a].

Obsoletes RFC0989 [?]. Status: UNKNOWN.

RFC1040

[Lin88b] J. Linn. RFC 1040: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures, January 1, 1988. URL ftp://ftp.internic.net/rfc/rfc1040.txt; ftp://ftp.internic.net/rfc/rfc1113.txt; ftp://ftp.internic.net/rfc/rfc989.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1040.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1113.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc989.txt. Obsoleted by RFC1113 [Lin89b]. Obsoletes RFC0989 [Lin87]. Status: UNKNOWN.

Linn:1989:RPE

[Lin89a] J. Linn. RFC 1113: Privacy enhancement for Internet electronic mail: Part I — message encipherment and authentication procedures, August 1, 1989. URL ftp://ftp.internic.net/rfc/rfc1040.txt; ftp://ftp.internic.net/rfc/rfc1113.txt; ftp://ftp.internic.net/rfc/rfc1421.txt; ftp://ftp.internic.net/rfc/rfc989.txt; https://www.math.utah.edu/pub/rfc/rfc1040.txt; https://www.math.utah.edu/pub/rfc/rfc1113.txt; https://www.math.utah.edu/pub/rfc/rfc1421.txt; https://www.math.utah.edu/pub/rfc/rfc989.txt. Obsoleted by RFC1421 [Lin93a]. Obsoletes RFC0989, RFC1040 [?, Lin93a]. Status: HISTORIC.

RFC1113

[Lin89b] J. Linn. RFC 1113: Privacy enhancement for Internet electronic mail: Part I — message encipherment and authentication procedures, August 1, 1989. URL ftp://ftp.internic.net/rfc/rfc1040.txt; ftp://ftp.internic.net/rfc/rfc1113.txt; ftp://ftp.internic.net/rfc/rfc1421.txt; ftp://ftp.internic.net/rfc/rfc989.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1040.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1113.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1421.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc989.txt. Obsoleted by RFC1421 [Lin93b]. Obsoletes RFC0989, RFC1040 [Lin87, Lin88b]. Status: HISTORIC.

Linn:1993:RPE

[Lin93a] J. Linn. RFC 1421: Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures, February 1993. URL ftp://ftp.internic.net/rfc/rfc1113.txt; ftp://ftp.internic.net/rfc/rfc1421.txt; https://www.math.utah.edu/pub/rfc/rfc1113.txt; https://www.math.utah.edu/pub/rfc/rfc1421.txt. Obsoletes RFC1113 [Lin89a]. Status: PROPOSED STANDARD.

RFC1421

[Lin93b] J. Linn. RFC 1421: Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures, February 1993. URL ftp://ftp.internic.net/rfc/rfc1113.txt; ftp://ftp.internic.net/rfc/rfc1421.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1113.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1421.txt. Obsoletes RFC1113 [Lin89b]. Status: PROPOSED STANDARD.

Linn:1993:RCA

[Lin93c] J. Linn. RFC 1511: Common authentication technology overview, September 1993. URL ftp://ftp.internic.net/rfc/rfc1511.txt; https://www.math.utah.edu/pub/rfc/rfc1511.txt. Status: INFORMATIONAL.

Lin:1996:IRC

[Lin96a] Herbert Lin. Inside risks: Cryptography's role in securing information. *Communications of the Association for Computing Machinery*, 39(8):131, August 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Linn:1996:RKV

[Lin96b] J. Linn. RFC 1964: The Kerberos Version 5 GSS-API mechanism, June 1996. URL ftp://ftp.internic.net/rfc/rfc1964.txt; https://www.math.utah.edu/pub/rfc/rfc1964.txt. Status: PROPOSED STANDARD.

Linnartz:1998:TCC

[Lin98] J. P. M. G. Linnartz. The "ticket" concept for copy control based on embedded signalling. In Quisquater et al. [Q+98], pages 257–274. ISBN 3-540-65004-0. LCCN QA267.A1 L43 no.1485. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073152.html.

Lippit:1993:PIC

[Lip93] Yukio Lippit. Phantomic inscryptions: the cryptology of Abraham and Torok. Thesis (A.B., Honors in Literature), Harvard University, Cambridge, MA, USA, 1993. 69 pp.

Lipton:1994:CNF

[Lip94] R. J. Lipton. Coding for noisy feasible channels. In IEEE [IEE94a], pages 27–?? ISBN 0-7803-2761-6. LCCN QA276 .I54 1994. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/041222.html. IEEE Catalog No. 94TH8100.

Abeles:1998:KVC

[Lip98] Francine Abeles Stanley H. Lipson. The key-vowel cipher of Charles L. Dodgson. In Deavours et al. [DKK+98], pages 323–329. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Lipmaa:1999:ICM

[Lip99] H. Lipmaa. IDEA: a cipher for multimedia architectures? *Lecture Notes in Computer Science*, 1556: 248–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Litant:1987:BRC

[Lit87] Thomas F. Litant. Book review: *Computer Security: the Practical Issues in a Troubled World*, (Elsevier Science Publishers, Amsterdam 1985). *Operating Systems Review*, 21(1):3–5, January 1987. CODEN OSRED8. ISSN 0163-5980.

Lindsay:1997:BC

[LJWH97] Charles Lindsay, Derek Jacobi, Hugh Whitemore, and Andrew Hodges. Breaking the code, 1997. ISBN 1-56442-662-9. Based on the play of the same title by Hugh Whitemore, and on the book, “Alan Turing: the enigma”, by Andrew Hodges. Originally broadcast as an episode of the PBS television series, Mobil masterpiece theatre Credits: Director of photography, Robin Vidgeon ; editor, Laurence Mery-Clark ; introduced by Russell Baker Performers: Derek Jacobi, Alun Armstrong, Richard Johnson, Harold Pinter, Amanda Root, Prunella Scales The story of Alan Turing, British mathematical genius and designer of the computer that broke the German Enigma code during World War II, whose admittance to homosexuality at a time when it was illegal presented problems for him, for his family, for his colleagues, and for the State's preoccupation with national security Close-captioned.

Laih:1996:CEE

[LK96] C.-S. Laih and W.-C. Kuo. Cryptanalysis of the enhanced ElGamal's signature scheme. *Lecture Notes in Computer Science*, 1029: 228–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lee:1999:MRF

[LK99] H.-W. Lee and T.-Y. Kim. Message recovery fair blind signature. *Lecture Notes in Computer Science*, 1560: 97–111, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Landau:1994:CPP

[LKB+94] Susan Landau, Stephen Kent, Clinton C. Brooks, Scott Charney, Dorothy E. Denning, Whitfield Diffie, Anthony Lauck, Douglas Miller, Peter G. Neumann, and David L. Sobel. Crypto policy perspectives. *Communications of the Association for Computing Machinery*, 37(8):115–121, August 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/179726.html.

Linnartz:1998:MFA

[LKD98] Jean-Paul Linnartz, Ton Kalker, and Geert Depovere. Modelling the false alarm and missed detection rate for electronic watermarks. *Lecture Notes in Computer Science*, 1525: 329–343, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250329.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250329.pdf.

Lenstra:1993:DNF

[LL93a] A. K. Lenstra and H. W. Lenstra, Jr. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-57013-6 (New York), 3-540-57013-6 (Berlin). viii + 131 pp. LCCN QA3 .L35 v.1554.

Liaw:1993:OAA

[LL93b] Horng Twu Liaw and Chin Laung Lei. An optimal algorithm to assign cryptographic keys in a tree structure for access control. *BIT*, 33(1):46–56, March 1993. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL http://www.mai.liu.se/BIT/contents/bit33.html; http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&

volume=33&issue=1&spage=46.

Lim:1994:AMA

[LL94a] Chae Hoon Lim and Pil Joong Lee. Another method for attaining security against adaptively chosen ciphertext attacks. *Lecture Notes in Computer Science*, 773: 420–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730420.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730420.pdf.

Lim:1994:MFE

[LL94b] Chae Hoon Lim and Pil Joong Lee. More flexible exponentiation with precomputation. In Desmedt [Des94b], pages 95–107. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390095.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390095.pdf.

Lim:1995:SPS

[LL95a] Chae Hoon Lim and Pil Joong Lee. Security and performance of server-aided RSA computation protocols. *Lecture Notes in Computer Science*, 963:70–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630070.htm; http://link.springer-ny.com/link/service/series/0558/papers/0963/09630070.pdf.

Lim:1995:SPP

[LL95b] Chae Hoon Lim and Pil Joong Lee. Several practical protocols for authentication and key exchange. *Information Processing Letters*, 53(2): 91–96, January 27, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lee:1997:PNB

[LL97a] Gang-Soo Lee and Jin-Seok Lee. Petri net based models for specification and analysis of cryptographic protocols. *The Journal of Systems and Software*, 37(2): 141–??, ???? 1997. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Lim:1997:DSA

[LL97b] Chae Hoon Lim and Pil Joong Lee. Directed signatures and application to threshold cryptosystems. *Lecture Notes in Computer Science*, 1189:131–138, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lim:1998:SPK

[LL98a] Chae Hoon Lim and Pil Joong Lee. A study on the proposed Korean Digital Signature Algorithm. *Lecture Notes in Computer Science*, 1514:175–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lin:1998:CDE

[LL98b] Chu-Hsing Lin and Tien-Chi Lee. A confused document encrypting scheme and its implementation. *Computers and Security*, 17 (6):543–551, ???? 1998. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404898800941`.

Lee:1999:NAD

[LL99] C.-H. Lee and J.-I. Lim. A new aspect of dual basis for efficient field arithmetic. *Lecture Notes in Computer Science*, 1560:12–28, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Langelaar:1998:RSS

[LLB98] G. C. Langelaar, R. L. Lagendijk, and J. Biemond. Removing spatial spread spectrum watermarks by non-linear filtering. In Theodoridis et al. [T+98], pages 2281–2284. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073147.html`. Four volumes.

Luo:2010:PAE

[LLG10] Yiyuan Luo, Xuejia Lai, and Zheng Gong. Pseudorandomness analysis of the (extended) Lai–Massey scheme. *Information Processing Letters*, 111(2):90–96, December 31, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [LM91a].

Laih:1989:NTS

[LLH89] Chi Sung Laih, Jau Yien Lee, and Lein Harn. A new threshold scheme and its application in designing the conference key distribution cryptosystem. *Information Processing Letters*, 32(3): 95–99, August 24, 1989. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lam:1996:EGE

[LLH96] Kwok-Yan Lam, San Ling, and Lucas C.-K. Hui. Efficient generation of elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 1090:411–416, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lenstra:1990:NFS

[LLMP90] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard. The number field sieve. In ACM [ACM90], pages 564–572. ISBN 0-89791-361-2. LCCN QA76.A15 1990. For discussion of the generalized number field sieve, see [LLMP93].

Lenstra:1993:FNF

[LLMP93] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard. The factorization of the ninth Fermat number. *Mathematics of Computation*, 61 (203):319–349, July 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). See [LLMP90].

Langie:1922:C

[LM22] André Langie and James Cruickshank Henderson Macbeth. *Cryptography.* Constable and Company Limited, London, UK, 1922. vii + 1 + 192 pp. LCCN Z 104 L26dE. Bibliography: p.158.

Luccio:1980:CMC

[LM80] F. Luccio and S. Mazzone. A cryptosystem for multiple communication. *Information Processing Letters*, 10 (4–5):180–183, July 5, 1980. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See notes [Mei81, Hel81].

Lidl:1984:PPR

[LM84] Rudolf Lidl and Winfried B. Müller. Permutation polynomials in RSA-cryptosystems. In *Advances in cryptology (Santa Barbara, Calif., 1983)*, pages 293–301. Plenum, New York, 1984.

Leighton:1985:HBC

[LM85] Albert C. Leighton and Stephen M. Matyas. The history of book ciphers. In Blakley and Chaum [BC85], pages 101–113. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=101`. CRYPTO 84: a Workshop on the Theory and Application of

Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Lai:1991:PNB

[LM91a] Xuejia Lai and James L. Massey. A proposal for a new block encryption standard. In *Advances in cryptology—EUROCRYPT '90 (Aarhus, 1990)*, volume 473 of *Lecture Notes in Computer Science*, pages 389–404. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730389.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730389.pdf`. See [LLG10] for proofs of requirements on the number of rounds.

Lia:1991:PNB

[LM91b] Xuejia Lia and James L. Massey. A proposal for a new block encryption standard. In Damgård [Dam91a], pages 55–70. CODEN LNCSD9. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1990. DM69.00.

Lai:1993:HFBa

[LM93a] X. Lai and J. L. Massey. Hash functions based on block ciphers. In Rueppel [Rue93], pages 53–66. CODEN LNCSD9. ISBN 0-387-56413-6 (New York), 3-540-56413-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1992.

Lai:1993:HFBb

[LM93b] Xuejia Lai and James L. Massey. Hash functions based on block ciphers. *Lecture Notes in Computer Science*, 658:55–70, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580055.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580055.pdf`.

Longley:1993:TNC

[LM93c] D. Longley and S. M. Matyas. Technical note: Complementarity attacks and control vectors. *IBM Systems Journal*, 32(2): 321–325, 1993. CODEN IBMSA7. ISSN 0018-8670.

Leighton:1994:SAP

[LM94a] Tom Leighton and Silvio Micali. Secret-key agreement without public-key cryptography. *Lecture*

Notes in Computer Science, 773:456–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Leighton:1994:SKA

[LM94b] Tom Leighton and Silvio Micali. Secret-key agreement without public-key cryptography. *Lecture Notes in Computer Science*, 773:456–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730456.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730456.pdf`.

Leighton:1995:LPF

[LM95] F. T. Leighton and S. Micali. Large provably fast and secure digital signature schemes from secure hash functions. US Patent 5,432,852., 1995.

Low:1996:MCP

[LM96] S. H. Low and N. F. Maxemchuk. Modeling cryptographic protocols and their collusion analysis. *Lecture Notes in Computer Science*, 1174:169–184, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054447.html`.

Lamersdorf:1998:TDS

[LM98a] Winfried Lamersdorf and Michael Merz, editors. *Trends in distributed systems for electronic commerce: international IFIP/GI working conference, TREC'98, Hamburg, Germany, June 3–5, 1998, proceedings*, volume 1402 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-64564-0 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1402.

Low:1998:PCT

[LM98b] S. H. Low and N. F. Maxemchuk. Performance comparison of two text marking methods. *IEEE Journal on Selected Areas in Communications*, 16(4): 561–572, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072132.html`.

Low:1995:DMI

[LMBO95] S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O'Gorman. Document marking and identification using both line and word shifting. In IEEE [IEE95c], pages 853–860. ISBN 0-7803-2525-7 (microfiche). ISSN 0743-166X. LCCN TK 5105.5 I33 1995. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1039.html. Three volumes. IEEE catalog number 95CH35759. IEEE Computer Society Press order number PR06990.

Le:1993:PKE

[LMJW93] A. V. Le, S. M. Matyas, D. B. Johnson, and J. D. Wilkins. A public key extension to the Common Cryptographic Architecture. *IBM Systems Journal*, 32(3):461–485, 1993. CODEN IBMSA7. ISSN 0018-8670. G321-5521.

Low:1998:DIC

[LML98] S. H. Low, N. F. Maxemchuk, and A. P. Lapone. Document identification for copyright protection using centroid detection. *IEEE Transactions on Communications*, 46(3):372–383, March 1998. CODEN IECMBT. ISSN 0090-6778 (print), 1558-0857 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/071150.html.

Lai:1991:MCD

[LMM91] X. Lai, J. L. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. *Lecture Notes in Computer Science*, 547:17–38, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lai:1992:MCD

[LMM92] X. Lai, J. L. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. In ????, editor, *Advances in Cryptology, Proceedings of EUROCRYPT 91*, volume 547 of *Lecture Notes in Computer Science*, pages 17–38. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992.

Lee:1999:DPP

[LMP99] H. Lee, K.-A. Moon, and J.-W. Park. Design of a parallel processing system for facial image retrieval. *Lecture Notes in Computer Science*, 1557:592–593, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Longo:1990:GCC

[LMS90] G. Longo, M. Marchi, and A. Sgarro. *Geometries, codes and cryptography*, volume 313 of *Courses and lectures*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 3-211-82205-4 (Wien), 0-387-

82205-4 (New York). 227 pp. LCCN Z103 .G46 1990. Based on lectures held at the International Centre for Mechanical Sciences in Udine, Italy, 1989.

Leonard:1997:CSP

[LMS97] J. Leonard and W. H. Mangione-Smith. A case study of partially evaluated hardware circuits: Key-specific DES. *Lecture Notes in Computer Science*, 1304: 151–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lautemann:1999:DCA

[LMSV99] C. Lautemann, P. McKenzie, T. Schwentick, and H. Vollmer. The descriptive complexity approach to LOGCFL. *Lecture Notes in Computer Science*, 1563: 444–454, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lidl:1994:IFF

[LN94] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, UK, revised edition, 1994. ISBN 0-521-46094-8 (hardback). xi + 416 pp. LCCN QA247.3 .L54 1994. URL ftp://uiarchive.cso.uiuc.edu/pub/etext/gutenberg/; http://www.loc.gov/catdir/description/cam026/93049020.html; http://www.loc.gov/catdir/samples/cam031/93049020.html; http://www.loc.gov/catdir/toc/cam029/93049020.html.

Lehti:1998:CT

[LN98] I. Lehti and P. Nikander. Certifying trust. *Lecture Notes in Computer Science*, 1431:83–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lagarias:1985:SLD

[LO85] J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *Journal of the Association for Computing Machinery*, 32(1):229–246, January 1985. CODEN JACOAH. ISSN 0004-5411. URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/2461.html. Preliminary version in *Proc. 24th IEEE Foundations Computer Science Symp.*, pp. 1–10, 1983.

LaMacchia:1991:CDL

[LO91a] B. A. LaMacchia and A. M. Odlyzko. Computation of discrete logarithms in prime fields. *Lecture Notes in Computer Science*, 537: 616–618, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.research.att.com/~amo/doc/arch/prime.discrete.logs.pdf; http://www.research.att.com/~amo/doc/arch/prime.discrete.logs.ps; http://www.research.att.com/~amo/doc/arch/prime.discrete.logs.tex.

LaMacchia:1991:SLS

[LO91b] B. A. LaMacchia and A. M. Odlyzko. Solving large sparse linear systems over finite fields. *Lecture Notes in Computer Science*, 537: 109–133, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.research.att.com/~amo/doc/arch/sparse.linear.eqs.pdf; http://www.research.att.com/~amo/doc/arch/sparse.linear.eqs.ps; http://www.research.att.com/~amo/doc/arch/sparse.linear.eqs.tex.

Lomet:1983:HPU

[Lom83] David B. Lomet. A high performance, universal, key associative access method. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 13 (4):120–133, May 1983. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Lomas:1994:ENT

[Lom94] M. Lomas. Encrypting network traffic. *Lecture Notes in Computer Science*, 809:64–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lomas:1997:SPI

[Lom97] Mark Lomas, editor. *Security protocols: international workshop: Cambridge, United Kingdom, April 10–12, 1996, proceedings*, volume 1189 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-62494-5 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C826 1997.

Long:1991:PAA

[Lon91] Yong Hong Long. A probabilistic attack algorithm for the public key cryptosystem RSA. *Natural Science Journal of Xiangtan University = Xiangtan Daxue Ziran Kexue Xuebao*, 13(3): 113–118, 1991. CODEN XDZEWR. ISSN 1000-5900. In Chinese.

Long:1992:UDE

[Lon92] Yong Hong Long. Using Diophantine equations to construct public-key cryptosystems. *Natural Science Journal of Xiangtan University = Xiangtan Daxue Ziran Kexue Xuebao*, 14(2): 116–122, 1992. CODEN XDZEWR. ISSN 1000-5900.

Loshin:1997:CGP

[Los97] Pete Loshin. Cryptography gets personal — six products that promise to secure your data, both over the Internet and on your desktop. *BYTE Magazine*, 22(11): 121–??, November 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Loshin:1998:PEC

[Los98] Peter Loshin. *Personal encryption clearly explained*. AP Professional, Boston, MA, USA, 1998. ISBN 0-12-455837-2 (paperback). xiii + 545 pp. LCCN QA76.9.A25 L67 1998.

Lowe:1995:ANS

[Low95] Gavin Lowe. An attack on the Needham–Schroeder public-key authentication protocol. *Information Processing Letters*, 56(3):131–133, November 10, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lowe:1996:BFN

[Low96] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. *Lecture Notes in Computer Science*, 1055: 147–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Loxton:1990:NTC

[Lox90] J. H. Loxton, editor. *Number theory and cryptography*, volume 154 of *London Mathematical Society lecture note series*. Cambridge University Press, New York, NY, USA, 1990. ISBN 0-521-39877-0. LCCN Z103 .N845 1990. Papers presented at the 33rd Annual Meeting of the Australian Mathematical Society and at a Workshop on Number Theory and Cryptography in Telecommunications held at Macquarie University in Sydney from 29 June to 7 July 1989.

Lam:1999:ACA

[LOX99] Kwok Yan Lam, Eiji Okamato, and Chaoping Xing, editors. *Advances in cryptology — ASIACRYPT'99: International Conference on the Theory and Application of Cryptology and Information Security, Singapore, November 14–18, 1999: proceedings*, volume 1716 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66666-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 1999.

Luciano:1987:CCC

[LP87] Dennis Luciano and Gordon Prichett. Cryptology: From Caesar ciphers to public-key cryptosystems. *College Mathematics Journal*, 18(1):2–17, January 1987. CODEN ???? ISSN 0746-8342 (print), 1931-1346 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/07468342.1987.11973000`.

Leszczynski:1994:SDA

[LP94] H. Leszczynski and J. Pieniazek. On some difference analogues of PDEs with a delay. *Lecture Notes in Computer Science*, 879: 349–357, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Li:1999:CKA

[LP99] Chih-Hung Li and Josef Pieprzyk. Conference key agreement from secret sharing. *Lecture Notes in Computer Science*, 1587: 64–76, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1587/15870064.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1587/15870064.pdf`.

Nag-dban-blo-bzan-bstan-pai-rgyal-mtshan:1991:RDN

[lPNdbbbprm91] Lcan lun Pandita Nag-dban-blo-bzan-bstan-pa'i-rgyal mtshan. *Rgya dkar nag rgya ser Kasmira Bal Bod Hor gyi yi ge dan dpe ris rnam gran man ba: graphic tables of Indic and allied scripts with ornamental and cryptographic characters of Tibet*. Library of Tibetan Works and Archives, Dharamsala, India, 1991. 30 pp. LCCN A 2 523 753. Tibetan, Mongolian, Nepali, and several Indic languages; prefatory matters in English. Reproduced from a incomplete A-ba-ga Bsod-nams-kun-sdud-glin blockprints from the library of the 4th Sga-rje Khams-sprul Rinpoche.

Lacy:1998:IPP

[LQRS98] Jack Lacy, Schuyler R. Quackenbush, Amy Reibman, and James H. Snyder. Intellectual property protection systems and digital watermarking. *Lecture Notes in Computer Science*, 1525:158–168, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http:`

//link.springer-ny.com/link/service/series/0558/bibs/1525/15250158.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250158.pdf.

Luby:1986:PRP

[LR86] M. Luby and C. Rackoff. Pseudo-random permutation generators and cryptographic composition. In ACM [ACM86], pages 356–363. ISBN 0-89791-193-8. LCCN QA 76.6 A13 1986. URL http://www.acm.org/pubs/articles/proceedings/stoc/12130/p356-luby/p356-luby.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/12130/p356-luby/. ACM order number 508860.

Lagarias:1988:UEP

[LR88a] Jeffrey C. Lagarias and James A. Reeds. Unique extrapolation of polynomial recurrences. *SIAM Journal on Computing*, 17(2):342–362, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Luby:1988:HCP

[LR88b] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Lai:1996:AHH

[LR96] X. Lai and R. A. Rueppel. Attacks on the HKM/HFX cryptosystem. *Lecture Notes in Computer Science*, 1039:1–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lysyanskaya:1998:GBD

[LR98] A. Lysyanskaya and Z. Ramzan. Group blind digital signatures: a scalable solution to electronic cash. *Lecture Notes in Computer Science*, 1465:184–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lai:1993:FCC

[LRW93] X. Lai, R. A. Rueppel, and J. Woollven. A fast cryptographic checksum algorithm based on stream ciphers. *Lecture Notes in Computer Science*, 718:339–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lange:1925:TC

[LS25] André Lange and E. A. Soudart. *Traité de cryptographie. (French) [Treatise on cryptography]*. Librairie Félix Alcan, Paris, France, 1925. xii + 366 + vi pp. LCCN Z104 .L26 1925.

Lange:1981:TC

[LS81] André Lange and E. A. Soudart. *Treatise on cryptography*, volume 36 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1981. ISBN 0-89412-055-7 (paperback). xvi + 168 pp. LCCN Z104.L2613 1981. Translation of: Traite de cryptographie / par André Lange et E.-A. Soudart. “Plus many problems in French for the solver”.

Lu:1989:SCI

[LS89] W. P. Lu and M. K. Sundareshan. Secure communication in Internet environments: a hierarchical key management scheme for End-to-End encryption. *IEEE Transactions on Communications*, 37(10): 1014–1023, October 1, 1989. CODEN IECMBT. ISSN 0090-6778 (print), 1558-0857 (electronic).

Lloyd:1992:RPA

[LS92] B. Lloyd and W. Simpson. RFC 1334: PPP authentication protocols, October 1992. URL `ftp://ftp.internic.net/rfc/rfc1334.txt`; `ftp://ftp.internic.net/rfc/rfc1994.txt`; `https://www.math.utah.edu/pub/rfc/rfc1334.txt`; `https://www.math.utah.edu/pub/rfc/rfc1994.txt`. Obsoleted by RFC1994 [Sim96b]. Status: PROPOSED STANDARD.

Lin:1997:LNU

[LS97] B. Lin and S. J. Shepherd. LABYRINTH: a new ultra high speed stream cipher. *Lecture Notes in Computer Science*, 1355:192–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lasker:1998:ACC

[LS98a] G. E. (George Eric) Lasker and Timothy K. Shih, editors. *Advances in computer cybernetics; multimedia computing and networking, multimedia presentation, interactive multimedia support systems, multiuser virtual worlds, platform architecture for multimedia tools, management schemes for collaborative computing, program transformation systems, cryptanalysis and cryptosystems, graph transformation framework, simulation based design and development, design and implementation of programming languages, object systems design, abstracting devices*. International Institute for Advanced Studies in Systems Research and Cybernetics, Windsor, ON, Canada, 1998. ISBN 0-921836-54-6. LCCN ????

Luby:1998:CBB

[LS98b] Michael Luby and Jessica Staddon. Combinatorial bounds for broadcast encryption. *Lecture Notes in Computer Science*, 1403: 512–526, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030512.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030512.pdf.

Lamport:1982:BGP

[LSP82] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4 (3):382–401, July 1982. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic). They proved that Byzantine agreement cannot be reached unless fewer than one-third of the processes are faulty. This result assumes that authentication, i.e., the crypting of messages to make them unforgeable, is not used. With unforgeable messages, they show that the problem is solvable for any $n \geq t > 0$, where n is the total number of processes and t is the number of faulty processes.

Livens:1995:CCI

[LSVV95] S. Livens, P. Scheunders, G. Van de Wouwer, and D. Van Dyck. Classification of corrosion images by wavelet signatures and LVQ networks. *Lecture Notes in Computer Science*, 970: 538–543, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Leung:1985:SCT

[LT85] A. K. Leung and S. E. Tavares. Sequence complexity as a test for cryptographic systems. In Blakley and Chaum [BC85], pages 468–474. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=468. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Leong:1991:UPE

[LT91] Philip Leong and Chris Tham. UNIX password encryption considered unsecure. In USENIX Association [USE91], pages 269–280. LCCN QA 76.76 O63 U84 1992.

Linnartz:1998:MPM

[LT98] J. P. M. G. Linnartz and J. C. Talstra. MPEG PTY-marks: Cheap detection of embedded copyright data in DVD-video. In Quisquater et al. [Q+98], pages 221–240. ISBN 3-540-65004-0. LCCN QA267.A1 L43 no.1485. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073151.html`.

Langley:1999:ACI

[LTEH99] P. Langley, C. Thompson, R. Elio, and A. Haddadi. An adaptive conversational interface for destination advice. *Lecture Notes in Computer Science*, 1652:347–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Laih:1995:SLF

[LTT95] Chi Sung Laih, Fu Kuan Tu, and Wen Chung Tai. On the security of the Lucas function. *Information Processing Letters*, 53(5):243–247, March 10, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lioen:1988:OMA

[LtW88a] W. Lioen, H. te Riele, and D. Winter. Optimization of the MPQS-factoring algorithm on the Cyber 205 and the NEC SX-2. *Supercomputer*, 5(4):42–50, July 1988. CODEN SPCOEL. ISSN 0168-7875.

Lioen:1988:OMF

[LtW88b] W. Lioen, H. te Riele, and D. Winter. Optimization of the MPQS-factoring algorithm on the Cyber 205 and the NEC SX-2. *Supercomputer*, 5(4):42–50, July 1988. CODEN SPCOEL. ISSN 0168-7875.

Lu:1979:EGC

[Lu79] Shyue Ching Lu. The existence of good cryptosystems for key rates greater than the message redundancy. *IEEE Transactions on Information Theory*, 25 (4):475–477, 1979. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Lu:1980:AEG

[Lu80] Shyue Ching Lu. Addition to: "The existence of good cryptosystems for key rates greater than the message redundancy" [IEEE Trans. Inform. Theory **25** (1979), no. 4, 475–477; MR

80g:94069]. *IEEE Transactions on Information Theory*, 26(1):129, 1980. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Lackey:1995:SMS

[LU95] R. J. Lackey and D. W. Upmal. Speakeasy: The military software radio. *IEEE Communications Magazine*, 33(5):56–61, May 1995. CODEN ICOMD9. ISSN 0163-6804. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/042155.html.

Luby:1996:PCA

[Lub96] Michael George Luby. *Pseudorandomness and cryptographic applications*. Princeton computer science notes. Princeton University Press, Princeton, NJ, USA, 1996. ISBN 0-691-02546-0. xvi + 234 pp. LCCN QA298 .L83 1996.

Lucks:1995:HEI

[Luc95] S. Lucks. How to exploit the intractability of exact TSP for cryptography. *Lecture Notes in Computer Science*, 1008:298–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lucks:1996:FLC

[Luc96a] S. Lucks. Faster Luby-Rackoff ciphers. *Lecture Notes in Computer Science*, 1039:189–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lucks:1996:FLR

[Luc96b] S. Lucks. Faster Luby-Rackoff ciphers. *Lecture Notes in Computer Science*, 1039:189–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lucks:1997:SRK

[Luc97] Stefan Lucks. On the security of remotely keyed encryption. *Lecture Notes in Computer Science*, 1267:219–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670219.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670219.pdf.

Lucks:1998:SBB

[Luc98a] S. Lucks. On the security of the 128-bit block cipher DEAL. Technical report, Universität Mannheim, Mannheim, Germany, August 20, 1998. URL http://th.informatik.uni-mannheim.de/m/lucks/papers/deal.ps.gz.

Lucks:1998:OKE

[Luc98b] S. Lucks. Open key exchange: How to defeat dictionary attacks without encrypting public keys. *Lecture Notes in Computer Science*, 1361:79–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lucks:1998:ATE

[Luc98c] Stefan Lucks. Attacking triple encryption. In Vaudenay [Vau98e], pages 239–253. CODEN LNCSD9. ISBN 3-540-64265-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25F77 1998. URL http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720239.htm; http://link.springer-ny.com/link/service/series/0558/papers/1372/13720239.pdf.

Lucks:1999:SBB

[Luc99a] S. Lucks. On the security of the 128-bit block cipher DEAL. *Lecture Notes in Computer Science*, 1636:60–70, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lucks:1999:SBC

[Luc99b] S. Lucks. On the security of the 128-bit block cipher DEAL. In Knudsen [Knu99c], pages 60–70. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Lucks:1999:ARK

[Luc99c] Stefan Lucks. Accelerated remotely keyed encryption. In Knudsen [Knu99c], pages 112–123. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1636/16360112.htm; http://link.springer-ny.com/link/service/series/0558/papers/1636/16360112.pdf.

Ludwig:1997:CQA

[Lud97] B. Ludwig. A contribution to the question of authenticity of Rhesus using part-of-speech-tagging. *Lecture Notes in Computer Science*, 1303:231–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lujan:1998:AMDa

[Luj98a] Susan M. Lujan. Agnes Meyer Driscoll. *Cryptolog*, ??(??):??, August 1998. ISSN 0740-7602.

Lujan:1998:AMDb

[Luj98b] Susan M. Lujan. Agnes Meyer Driscoll. In Deavours et al. [DKK+98], pages 269–

278. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Lunt:1990:EK

[Lun90] Steven Lunt. Experiences with Kerberos. In USENIX Association [USE90], pages 113–120. LCCN QA 76.9 A25 U55 1990.

Lutz:1998:NBM

[Lut98] Michael J. Lutz. New books: Making wavelets in the real world; protecting the OB; Diffie on privacy; digital design explained; E-commerce du jour; seeing software; structures for XML; Smalltalk patterns. *Computer*, 31 (6):97, June 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co1998/pdf/r6097.pdf.

Linnartz:1998:ASA

[LvD98] Jean-Paul M. G. Linnartz and Marten van Dijk. Analysis of the sensitivity attack against electronic watermarks in images. *Lecture Notes in Computer Science*, 1525:258–272, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250258.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250258.pdf.

Langelaar:1996:CPM

[LvdLB96] G. C. Langelaar, J. C. A. van der Lubbe, and J. Biemond. Copy protection for multimedia data based on labeling techniques. In Heideman [Hei96a], pages 33–40. ISBN 90-365-0812-6. LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1038.html.

Langelaar:1997:RLM

[LvdLL97] G. C. Langelaar, J. C. A. van der Lubbe, and R. L. Lagendijk. Robust labeling methods for copy protection of images. In Sethi and Jain [SJ97], pages 298–309. ISBN 0-8194-2433-1. LCCN TS510.S63 v.3022. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/063145.html.

Long:1988:DLH

[LW88] Douglas L. Long and Avi Wigderson. The discrete logarithm hides $O(\log n)$ bits. *SIAM Journal on Computing*, 17(2):363–372, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Li:1991:JAE

[LW91] Y. Li and X. Wang. A joint authentication and encryption scheme based on algebraic coding theory. *Lecture Notes in Computer Science*, 539:241–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lervik:1996:IDS

[LW96] John M. Lervik and Patrick Waldemar, editors. *1996 IEEE Digital Signal Processing Workshop: proceedings, September 1–4, 1996, Hotel Alexandra, Loen, Norway (DSPWS-96)*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN 0-7803-3629-1 (softbound), 0-7803-3630-5 (microfiche), 82-993923-0-6 (Norway) (??invalid checksum??). LCCN TK5102.9.I3 1996. IEEE catalog number: 96TH8225.

Lucks:1999:RKE

[LW99] Stefan Lucks and Rüdiger Weis. Remotely keyed encryption using non-encrypting Smart Cards. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL `http://www.usenix.org/publications/library/proceedings/smartcard99/lucks.html`.

Lin:1996:GTU

[LWC96] C.-H. Lin, C.-T. Wang, and C.-C. Chang. A group-oriented (t, n) undeniable signature scheme without trusted center. *Lecture Notes in Computer Science*, 1172:266–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lenstra:1995:KES

[LWY95] Arjen K. Lenstra, Peter Winkler, and Yacov Yacobi. A key escrow system with warrant bounds. *Lecture Notes in Computer Science*, 963:197–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630197.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0963/09630197.pdf`.

Laih:1993:SAS

[LY93] C.-S. Laih and S.-M. Yen. Secure addition sequence and its applications on the server-aided secret computation protocols. *Lecture Notes in Computer Science*, 718:219–??, 1993. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lodge:1994:SCC

[LYG94] J. Lodge, R. Young, and P. Guinand. Separable concatenated codes with iterative map filtering. *Lecture Notes in Computer Science*, 793:223–240, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Laih:1993:TES

[LYH93] Chi-Sung Laih, Sung-Ming Yen, and Lein Harn. Two efficient server-aided secret computation protocols based on the addition sequence. *Lecture Notes in Computer Science*, 739: 450–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Li:1990:ACP

[LZ90] Da Xing Li and Ze Zeng Zhang. An attack on a class of public key cryptosystems based on the Euclidean algorithm. *Kexue Tongbao (Chinese)*, 35(11):871–874, 1990. ISSN 0023-074X.

Li:1991:BCP

[LZ91a] Da Xing Li and Ze Zeng Zhang. Breaking a class of public-key cryptosystems with Euclid algorithm. *Chinese Sci. Bull.*, 36(10):873–876, 1991. ISSN 1001-6538.

Li:1991:HBM

[LZ91b] Da Xing Li and Ze Zeng Zhang. How to break up modified Lu-Lee cryptosystems. *Chinese Sci. Bull.*, 36 (12):1050–1053, 1991. ISSN 1001-6538.

Ma:1979:RAD

[Ma79] Robert Ma. Review and analysis of the Data Encryption Standard. Master of science, plan ii., Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA, 1979. 70 pp.

Meijer:1981:DSS

[MA81] Henk Meijer and Selim G. Akl. Digital signature schemes. Technical report 81-120, Department of Computing and Information Science, Queen's University, Kingston, ON, Canada, 1981. 10 pp.

MacPherson:1987:CUN

[Mac87] B. Nelson MacPherson. The compromise of US Navy cryptanalysis after the Battle of Midway. *Intelligence and National Security*, 2 (2):320–??, 1987. ISSN 0268-4527 (print), 1743-9019 (electronic).

MacLaren:1994:CPN

[Mac94] N. MacLaren. Cryptographic pseudorandom numbers in simulation. *Lecture Notes in Computer Science*, 809:185–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mache:1998:SCT

[Mac98] Wolfgang W. Mache. The Siemens cipher teletype in the history of telecommunications. In Deavours et al. [DKK+98], pages 433–453. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Madsen:1992:GCD

[Mad92] Jørgen Bo Madsen. The greatest cracker-case in Denmark: The detecting, tracing, and arresting of two international crackers. In USENIX [USE92b], pages 17–40. ISBN 1-880446-46-4. LCCN ????

Madsen:1996:CCL

[Mad96] Wayne Madsen. Congressional Committee looks at US encryption policy. *Network Security*, 1996(12):7–8, December 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896900872.

Madsen:1997:KEE

[Mad97] Wayne Madsen. Key Escrow Encryption Bill hits Congress. *Network Security*, 1997(7):11–12, July 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897898819.

Madsen:1998:CPH

[Mad98a] Wayne Madsen. Crypto politics heating up. *Network Security*, 1998(8):5–6, August 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898800706.

Madsen:1998:CPU

[Mad98b] Wayne Madsen. Cryptography protected under US constitution. *Network Security*, 1998(1):7–8, January 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898901647.

Madsen:1998:EDR

[Mad98c] Wayne Madsen. Encryption debate rages again. *Network Security*, 1998(5):8–9, May 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898801190.

Madsen:1998:ELP

[Mad98d] Wayne Madsen. Encryption legislation and policy. *Network Security*, 1998(7): 6–7, July 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898800056.

Madsen:1998:FFE

[Mad98e] Wayne Madsen. Family feud over encryption policy. *Network Security*, 1998(6): 5–6, June 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898900071.

Madsen:1998:NCK

[Mad98f] Wayne Madsen. NAFTA has crypto key recovery agenda. *Network Security*, 1998(7):7–8, July 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898900411.

Madsen:1998:USC

[Mad98g] Wayne Madsen. Uncle Sam's crypto road show. *Network Security*, 1998(3): 8–13, March 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800875959.

Madsen:1999:MBF

[Mad99a] Wayne Madsen. McCain's bill further 'Balkanizes' US crypto export policy. *Network Security*, 1999(5):6–7, May 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899902878.

Madsen:1999:NCO

[Mad99b] Wayne Madsen. NSA continues to oppose crypto export control relief. *Network Security*, 1999(3):9–10, March 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899900260.

Maes:1998:TPH

[Mae98] Maurice Maes. Twin Peaks: The histogram attack to fixed depth image watermarks. *Lecture Notes in Computer Science*, 1525: 290–305, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250290.htm; http://link.springer-

ny.com/link/service/series/0558/papers/1525/15250290.pdf.

Maher:1996:CBK

[Mah96] David Paul Maher. Crypto backup and key escrow. *Communications of the Association for Computing Machinery*, 39(3):48–53, March 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/227241.html; http://www.acm.org/pubs/toc/Abstracts/cacm/227241.html.

McDonald:1995:OTP

[MAM95] Daniel L. McDonald, Randall J. Atkinson, and Craig Metz. One-Time Passwords in Everything (OPIE): Experiences with building and using stronger authentication. In USENIX Association [USE95b], pages 177–186. ISBN 1-880446-70-7. LCCN QA76.8.U65 U55 1992(3)-1995(5). URL http://www.usenix.org/publications/library/proceedings/security95/mcdonald.html.

Mandelbrot:1960:BRJa

[Man60] Benoît Mandelbrot. Book review: John Chadwick, *The Decipherment of Linear B* (1958) Cambridge University Press. *Information and Control*, 3(1):95–96, March 1960. CODEN IFCNA4. ISSN 0019-9958 (print), 1878-2981 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0019995860903478.

Manasse:1995:MPE

[Man95] M. Manasse. The Millicent protocols for electronic commerce. ????, 1995. URL http://www.research.digital.com/SRC/millicent.

Manjunath:1998:IPA

[Man98] B. S. Manjunath. Image processing in the Alexandria Digital Library project. In IEEE [IEE98d], pages 180–187. ISBN 0-8186-8464-X, 0-8186-8466-6 (microfiche). LCCN TK5103.5.F678 1998. IEEE Computer Society Press Order Number PR08464. IEEE Order Plan Catalog Number 98TB100235.

Moriai:1996:KLP

[MAO96] Moriai, K. Aoki, and K. Ohta. Key-dependency of linear probability of RC5. To appear in IEICE Trans. Fundamentals., March 1996.

Mao:1997:PVP

[Mao97] W. Mao. Publicly verifiable partial key escrow. *Lecture Notes in Computer Science*, 1334:409–??, 1997. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Mao:1998:GCS

[Mao98] W. Mao. Guaranteed correct sharing of integer factorization with off-line shareholders. *Lecture Notes in Computer Science*, 1431: 60–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Marsh:1970:CSS

[Mar70a] D. C. B. Marsh. *Cryptology as a senior seminar topic*. Mathematical Association of America, Buffalo, NY, USA, 1970. 761–764 pp. Reprint from American Mathematical Monthly, vol. 77, no. 7, August-September, 1970.

Marsh:1970:MEC

[Mar70b] D. C. B. Marsh. Mathematical education: Cryptology as a senior seminar topic. *American Mathematical Monthly*, 77(7):761–764, August/September 1970. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Marion:1976:ANB

[Mar76] Bruce Phillip Marion. Analysis of National Bureau of Standards Data Encryption Algorithm. Thesis (Engineer), Department of Electrical Engineering, Stanford University, Stanford, CA, USA, 1976. v + 46 pp.

Marion:1995:WGT

[Mar95a] Larry Marion. Who's guarding the till at the CyberMall? *Datamation*, 41(3):38–41, February 15, 1995. CODEN DTMNAT. ISSN 0011-6963.

Marks:1995:PEI

[Mar95b] Richard D. Marks. *Protecting enterprise information in the digital age: encryption, digital telephony, privacy and security*. American Bar Association, Science and Technology Section, Chicago, IL, USA, 1995. various pp.

Markoff:1996:MIS

[Mar96] John Markoff. The microprocessor's impact on society — at 25 years old, has the microprocessor fulfilled its early promise? what does it offer for the future? *IEEE Micro*, 16(6):54–59, November/December 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Martin:1997:IEI

[Mar97] K. M. Martin. Increasing efficiency of international key escrow in mutually mistrusting domains. *Lecture Notes in Computer Science*, 1355:221–??, 1997. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Markantonakis:1998:CSM

[Mar98a] C. Markantonakis. The case for a secure multi-application smart card operating system. *Lecture Notes in Computer Science*, 1396:188–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Marks:1998:BSC

[Mar98b] Leo Marks. *Between silk and cyanide: a codemaker's war, 1941–1945*. Free Press, New York, NY, USA, 1998. ISBN 0-684-86422-3. 613 pp. LCCN D810.C88 M375 1999. URL http://www.loc.gov/catdir/bios/simon054/99017581.html; http://www.loc.gov/catdir/description/simon032/99017581.html; http://www.loc.gov/catdir/enhancements/fy0705/99017581-s.html; http://www.loc.gov/catdir/enhancements/fy0705/99017581-t.html.

Martyna:1999:NNA

[Mar99] J. Martyna. Neural network approach to design of distributed hard real-time systems. *Lecture Notes in Computer Science*, 1625: 118–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Massey:1983:LFC

[Mas83] J. L. Massey. Logarithms in finite cycle groups – cryptographic issues. In Edward C. van der Meulen, editor, *Proceedings of the Fourth Symposium on Information Theory in the Benelux: held at the Brembergcentrum, Haasrode, Belgium, May 26–27, 1983*, pages 17–25. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1983. ISBN 90-334-0690-X. LCCN Q350 S988 1983.

Mastrovito:1989:VDM

[Mas89] E. D. Mastrovito. VLSI designs for multiplication over finite fields GF(2^m). *Lecture Notes in Computer Science*, 357:397–309, 1989. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mastrovito:1991:VAC

[Mas91] E. D. Mastrovito. *VLSI Architectures for Computations in Galois Fields*. Ph.D. thesis, Linköping University, Linköping, Sweden, 1991. ???? pp.

Massey:1994:SKB

[Mas94] J. Massey. SAFER K-64: a byte-oriented block-ciphering algorithm. *Lecture Notes in Computer Science*, 809:1–??, 1994.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Massacci:1997:BSP

[Mas97] Massacci. Breaking security protocols as an AI planning problem. *Lecture Notes in Computer Science*, 1348: 286–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Massacci:1999:DRT

[Mas99a] F. Massacci. Design and results of the Tableaux-99 non-classical (modal) systems comparison. *Lecture Notes in Computer Science*, 1617:14–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Massey:1999:OSD

[Mas99b] James Massey. On the optimality of SAFER+ diffusion. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Matyas:1979:DSO

[Mat79] Stephen M. Matyas. Digital signatures — an overview. *Computer Networks: The International Journal of Distributed Informatique*, 3 (2):87–94, April 1979. CODEN CNETDP. ISSN 0376-5075.

Matyas:1991:KHC

[Mat91] S. M. Matyas. Key handling with control vectors. *IBM Systems Journal*, 30 (2):151–174, 1991. CODEN IBMSA7. ISSN 0018-8670.

Matsui:1993:LCM

[Mat93] M. Matsui. Linear cryptanalysis method for DES cipher. *Lecture Notes in Computer Science*, 765: 386–397, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Matsui:1994:FEC

[Mat94a] Mitsuru Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In Desmedt [Des94b], pages 1–11. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390001.htm; http://link.springer-

ny.com/link/service/series/0558/papers/0839/08390001.pdf.

Matsui:1994:LCM

[Mat94b] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Helleseth [Hel94], pages 386–397. CODEN LNCSD9. ISBN 3-540-57600-2 (Berlin), 0-387-57600-2 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1993. DM86.00. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0765.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=765.

Matsui:1995:CBO

[Mat95] M. Matsui. On correlation between the order of S-boxes and the strength of DES. *Lecture Notes in Computer Science*, 950: 366–375, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Matsui:1996:NSB

[Mat96a] M. Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. *Lecture Notes in Computer Science*, 1039: 205–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Matthews:1996:SRN

[Mat96b] Tim Matthews. Suggestions for random number generation in software. *RSA Laboratories' Bulletin*, 1:1–4, January 22, 1996. URL ftp://ftp.rsasecurity.com/pub/pdfs/bull-1.pdf.

Matsui:1997:NBE

[Mat97] Mitsuru Matsui. New block encryption algorithm MISTY. *Lecture Notes in Computer Science*, 1267: 54–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670054.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670054.pdf.

Matsumoto:1998:HCC

[Mat98] Tsutomu Matsumoto. Human–computer cryptography: An attempt. *Journal of Computer Security*, 6(3): 129–149, ???? 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Matsumura:1999:DTE

[Mat99] T. Matsumura. Description of team erika. *Lecture Notes in Computer Science*, 1604:377–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mauborgne:1914:APC

[Mau14] Joseph O. Mauborgne. An advanced problem in cryptography and solution. Technical report, Army Service School's Press, Ft. Leavenworth, KS, USA, 1914. 21 pp.

Maurer:1990:FGS

[Mau90] Ueli M. Maurer. Fast generation of secure RSA-moduli with almost maximal diversity. *Lecture Notes in Computer Science*, 434:636–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340636.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340636.pdf`.

Maurer:1991:NAD

[Mau91a] U. M. Maurer. New approaches to the design of self-synchronizing stream ciphers. *Lecture Notes in Computer Science*, 547:458–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Maurer:1991:DSS

[Mau91b] Ueli M. Maurer. A digital signature scheme and a public-key cryptosystem based on elliptic curves over Z[subscript m]. DIMACS technical report 91-39, DIMACS, Center for Discrete Mathematics and Theoretical Computer Science, Rutgers, NJ, USA, May 1991. 11 pp.

Maurer:1991:PCS

[Mau91c] Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In ACM [ACM91], pages 561–571. ISBN 0-89791-397-3. LCCN QA 76.6 A13 1991. URL `http://www.acm.org/pubs/articles/proceedings/stoc/103418/p561-maurer/p561-maurer.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/103418/p561-maurer/`. IEEE Computer Society order no. 2190.

Maurer:1991:PSS

[Mau91d] Ueli M. Maurer. A provably-secure strongly-randomized cipher. *Lecture Notes in Computer Science*, 473:361–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730361.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730361.pdf.

Maurer:1993:PSK

[Mau93a] U. M. Maurer. Protocols for secret key agreement by public discussion based on common information. *Lecture Notes in Computer Science*, 740:461–470, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Maurer:1993:RIT

[Mau93b] U. M. Maurer. The role of information theory in cryptography. In Farrell [Far93], pages 49–71. ISBN 0-905091-03-5. LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/041815.html.

Maurer:1994:TEB

[Mau94] Ueli M. Maurer. Towards the equivalence of breaking the Diffie–Hellman protocol and computing discrete logarithms. In Desmedt [Des94b], pages 271–281. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390271.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390271.pdf.

Maurer:1996:UGT

[Mau96a] U. M. Maurer. A unified and generalized treatment of authentication theory. *Lecture Notes in Computer Science*, 1046:387–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Maurer:1996:ACE

[Mau96b] Ueli Maurer, editor. *Advances in cryptology, EUROCRYPT '96: International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12–16, 1996: proceedings*, volume 1070 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-61186-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1996. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1070.htm; http://www.springerlink.com/

openurl.asp?genre=issue&issn=0302-9743&volume=1070. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Maurer:1997:ITS

[Mau97a] Ueli M. Maurer. Information-theoretically secure secret-key agreement by NOT authenticated public discussion. In Fumy [Fum97], pages 209–225. CODEN LNCSD9. ISBN 3-540-62975-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1997. URL http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330209.htm; http://link.springer-ny.com/link/service/series/0558/papers/1233/12330209.pdf; http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/062815.html. Sponsored by the International Association for Cryptologic Research (IACR).

Mauriello:1997:TTC

[Mau97b] Ermelindo Mauriello. TCFS: Transparent cryptographic file system. *Linux Journal*, 40:??, August 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL ftp://ftp.ssc.com/pub/lj/listings/issue40/2174.tgz.

Mauth:1997:SOC

[Mau97c] Rainer Mauth. Steganography overcomes cryptography restrictions. *BYTE Magazine*, ??(??):??, January 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic). URL http://www.byte.com/art/9701/sec18/art2.htm.

Maurer:1998:E

[Mau98] U. Maurer. Eurocrypt '96. *Lecture Notes in Computer Science*, 1440: 199–206, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Maurer:1999:IC

[Mau99a] U. Maurer. Information-theoretic cryptography. In Wiener [Wie99], pages 47–64. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Maurer:1999:ITC

[Mau99b] U. Maurer. Information-theoretic cryptography. *Lecture Notes in Computer Science*, 1666:47–64, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Maxemchuk:1994:EDD

[Max94] N. F. Maxemchuk. Electronic document distribution. *AT&T Technical Journal*, 73(5):73–80, September/October 1994. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/034157.html`.

May:1997:CDS

[May97] Anneliese May. Comparison of digital signature legislation. Technical report, National Conference of State Legislatures, Washington, DC, USA, April 1997. v + 42 pp.

Milner-Barry:1986:ADL

[MB86] P. S. Milner-Barry. 'Action This Day': The letter from Bletchley Park cryptanalysts to the Prime Minister, 21 October 1941. *Intelligence and National Security*, 1(2):??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Mao:1994:SAP

[MB94a] W. Mao and C. Boyd. On strengthening authentication protocols to foil cryptanalysis. *Lecture Notes in Computer Science*, 875: 193–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Massey:1994:CCT

[MB94b] James L. Massey and Richard E. Blahut. *Communications and cryptography: two sides of one tapestry*. The Kluwer international series in engineering and computer science; Communications and information theory. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1994. ISBN 0-7923-9469-0. xvi + 481 pp. LCCN TK5102.94 .C64 1994. Talks presented at the Symposium on 'Communications, Coding, and Cryptography' in honor of James L. Massey on the occasion of his 60th birthday, Centro Stefano Franscini, Ascona, Switzerland, February 10–14, 1994.

Mehrotra:1999:NOA

[MB99a] Rajiv Mehrotra and Robin Baldwin. In the news: Online auctions attract buyers; xDSL reaches out and touches someone; business trends; Lucent delivers IP telephony; MP3: Dividing communities; the net attracts top musicians; service-level agreements reassure small businesses; digital signature for GSM phones; voice XML forum created. *IEEE MultiMedia*, 6(2):4–8, April–June 1999. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL http://dlib.computer.org/mu/books/mu1999/pdf/u2004.pdf.

Mitra:1999:DCT

[MB99b] N. Mitra and R. Brennan. Design of the CORBA/TC inter-working gateway. *Lecture Notes in Computer Science*, 1597:84–100, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mintzer:1998:OWS

[MBB98] Fred Mintzer, Gordon W. Braudaway, and Alan E. Bell. Opportunities for watermarking standards. *Communications of the Association for Computing Machinery*, 41(7):57–64, July 1998. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org:80/pubs/citations/journals/cacm/1998-41-7/p57-mintzer/; http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073154.html.

Murphy:1997:ROD

[MBW97] S. Murphy, M. Badger, and B. Wellington. RFC 2154: OSPF with digital signatures, June 1997. URL ftp://ftp.internic.net/rfc/rfc2154.txt; https://www.math.utah.edu/pub/rfc/rfc2154.txt. Status: EXPERIMENTAL.

Mintzer:1997:EIDb

[MBY97] Fred Mintzer, Gordon W. Braudaway, and Minerva M. Yeung. Effective and ineffective digital watermarks. In IEEE [IEE97h], pages 9–12. ISBN 0-8186-8183-7, 0-8186-8184-5 (case). LCCN TK8315 .I16 1997. Three volumes. IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144.

Moskowitz:1992:CAA

[MC92] I. S. Moskowitz and O. L. Costich. A classical automata approach to noninterference type problems. In IEEE [IEE92a], pages 2–8. ISBN 0-8186-2850-2. LCCN QA 76.9 A25 C655 1992. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/021420.html. IEEE catalog number 92TH0447-3.

Mitchell:1996:CKU

[MC96] Chris J. Mitchell and Liqun Chen. Comments on the S/KEY user authentication scheme. *Operating Systems Review*, 30(4):12–16, October 1996. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

McCarthy:1975:AFP

[McC75] John McCarthy. ACM Forum: Proposed criterion for a cipher to be probable-word-proof. *Communications of the Association for Computing Machinery*, 18 (2):131–132, February 1975. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [FH74].

McCurley:1990:DLP

[McC90a] Kevin S. McCurley. The discrete logarithm problem. In Pomerance and Goldwasser [PG90], pages 49–74. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

McCurley:1990:OEC

[McC90b] Kevin S. McCurley. Odds and ends from cryptology and computational number theory. In Pomerance and Goldwasser [PG90], pages 145–166. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

McCurley:1996:CIL

[McC96] K. S. McCurley. Cryptography and the Internet: Lessons and challenges. *Lecture Notes in Computer Science*, 1163:50–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

McCane:1998:ICS

[MCD98a] B. McCane, T. Caelli, and O. De Vel. Inducing complex spatial descriptions in two dimensional scenes. *Lecture Notes in Computer Science*, 1359: 123–132, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Millan:1998:HDC

[MCD98b] W. Millan, A. Clark, and E. Dawson. Heuristic design of cryptographically strong balanced Boolean functions. *Lecture Notes in Computer Science*, 1403:489–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Millan:1999:BFD

[MCD99] W. Millan, A. Clark, and E. Dawson. Boolean function design using hill climbing methods. *Lecture*

Notes in Computer Science, 1587:1–11, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

McHugh:1992:EBD

[McH92] J. McHugh. An EMACS based downgrader for the SAT. In IEEE [IEE92b], pages 228–237. ISBN 0-8186-3115-5 (paperback), 0-8186-3116-3 (microfiche), 0-8186-3117-1 (casebound). LCCN QA76.9.A25 C6375 1992. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1013.html. Reprinted in 'Computer and Network Security'.

McIvor:1985:SC

[McI85] R. McIvor. Smart cards. *Scientific American*, 253(5): 130–137, November 1985. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

McKee:1999:SFF

[McK99] James McKee. Speeding Fermat's factoring method. *Mathematics of Computation*, 68(228):1729–1737, October 1999. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-99-01133-3&u=/mcom/1999-68-228/. This paper present an $O(N^{1/4+\epsilon})$ integer factoring algorithm that never requires arithmetic on numbers larger than the one to be factored.

McLaughlin:1992:YAM

[McL92] Robert McLaughlin. Yet another machine to break DES. *Computers and Security*, 11(5):492, September 1992. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740489290259T.

McMahon:1996:RGA

[McM96] P. McMahon. RFC 1961: GSS-API authentication method for SOCKS version 5, June 1996. URL ftp://ftp.internic.net/rfc/rfc1961.txt; https://www.math.utah.edu/pub/rfc/rfc1961.txt. Status: PROPOSED STANDARD.

Madson:1998:REC

[MD98] C. Madson and N. Doraswamy. RFC 2405: The ESP DES-CBC cipher algorithm with explicit IV, November 1998. URL ftp://ftp.internic.net/rfc/rfc2405.txt; https://www.math.utah.edu/pub/rfc/rfc2405.txt. Status: PROPOSED STANDARD.

Main:1999:HCB

[MD99] J. Main and T. S. Dillon. A hybrid case-based reasoner for footwear design. *Lecture*

Notes in Computer Science, 1650:497–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Moreno-Diaz:1994:SIE

[MDP94] Roberto Moreno-Diaz and Franz Pichler. *Special issue — Eurocast 1993 International Workshop on Computer Aided Systems Theory*, volume 25(1) of *Cybernetics and systems*. Taylor and Francis, Washington, DC, USA, 1994. ISSN 0196-9722. various pp.

Messerges:1999:IPA

[MDS99] Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan. Investigations of power analysis attacks on Smartcards. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL `http://www.usenix.org/publications/library/proceedings/smartcard99/messerges.html`.

Meador:1920:KCE

[Mea20] J. E. D. Meador. Keeping the camera on an even keel, telephoning in cipher. *Scientific American*, 123(5): 107, July 31, 1920. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.nature.com/scientificamerican/journal/v123/n5/pdf/scientificamerican07311920-107a.pdf`.

Meadows:1995:FVC

[Mea95] C. A. Meadows. Formal verification of cryptographic protocols: a survey. *Lecture Notes in Computer Science*, 917:133–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mead:1998:BJA

[Mea98] David Mead. The breaking of the Japanese Army Administrative Code. In Deavours et al. [DKK+98], pages 465–475. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Meek:1998:AAM

[Mee98] Jon Meek. Apache authentication module. *;login: the USENIX Association newsletter*, 23(3):??, May 1998. CODEN LOGNEM. ISSN 1044-6397. URL `http://www.usenix.org/publications/login/1998-5/meek.html`. Special issue on security.

Meersman:1999:SOT

[Mee99] R. A. Meersman. Semantic ontology tools in IS design. *Lecture Notes in Computer*

Science, 1609:30–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Meijer:1981:NCM

[Mei81] H. Meijer. A note on "A cryptosystem for multiple communication" [Inform. Process. Lett. **10**(4–5), 5 July 1980, pp. 180–183]. *Information Processing Letters*, 12(4):179–181, August 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [LM80, Hel81].

Meijer:1983:CCC

[Mei83] Henk Meijer. *Cryptology computational complexity and applications*. Thesis (Ph.D.), Queen's University, Ottawa, ON, Canada, 1983. 2 microfiches (179 fr.).

Meijer:1985:MEN

[Mei85] Henk Meijer. Multiplication-permutation encryption networks. Technical report 85-171, Department of Computing and Information Science, Queen's University, Kingston, Ont., Canada, 1985. 15 pp.

Meijer:1992:SSA

[Mei92] A. R. Meijer. *Sharing a secret: applications of number theory and set theory to cryptology*, volume 730 of *UMAP modules in undergraduate mathematics and its applications*. COMAP, Inc., Lexington, MA, USA, 1992. 12 pp.

Meier:1994:SIB

[Mei94] W. Meier. On the security of the IDEA block cipher. *Lecture Notes in Computer Science*, 765:371–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Meierhofer:1996:PGP

[Mei96a] Christine Meierhofer. Pretty good privacy. In Blau et al. [B$^+$96b], page 35. ISBN 0-89791-784-7. ISSN 1069-5419. LCCN T385 .S54 1996b. URL `http://www.acm.org:80/pubs/citations/proceedings/graph/253607/p35-meierhofer/`.

Meijer:1996:GFC

[Mei96b] A. R. Meijer. Groups, factoring, and cryptography. *Mathematics Magazine*, 69 (2):103–109, 1996. CODEN MAMGA8. ISSN 0025-570X.

Meinel:1998:HHB

[Mei98] Carolyn P. Meinel. How hackers break in ... and how they are caught: Port scanners, core dumps and buffer overflows are but a few of the many weapons in every sophisticated hacker's arsenal. still, no hacker is invincible. *Scientific Amer-*

ican, 279(4):98–105, October 1998. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Mendelsohn:1939:CC

[Men39] Charles Jastrow Mendelsohn. *Cardan on cryptography*. Yeshiva College, New York, NY, USA, 1939. 157–168 pp. LCCN ???? Reprinted from Scripta mathematica, Vol. 6, No. 3, October, 1939. J. S. Galland, Bibliography of ... cryptology, 1945, p. 124.

Mendelsohn:1989:CWI

[Men89] John Mendelsohn, editor. *Covert warfare: intelligence, counterintelligence, and military deception during the World War II era*. Garland, New York, NY, USA, 1989. ISBN 0-8240-7950-7 (vol. 1). ???? pp. LCCN D810.S7 C66 1989. US$60.00.

Mendez:1991:AKA

[Men91] Trevor D. (Trevor DeCordova) Mendez. Adding Kerberos authentication to the QUIPU implementation of X.500. Thesis (B.S.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1991. 24 pp.

Menezes:1993:ECP

[Men93] Alfred Menezes. *Elliptic Curve Public Key Cryptosystems*, volume 234 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, MA, 1993. ISBN 0-7923-9368-6. xiv + 128 pp. LCCN QA76.9.A25 M46 1993. With a foreword by Neal Koblitz, Communications and Information Theory.

Menezes:1995:ECC

[Men95a] Alfred Menezes. Elliptic curve cryptosystems. *CryptoBytes*, 1(2):1, 3–4, Summer 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf`.

Menicocci:1995:SAC

[Men95b] R. Menicocci. A systematic attack on clock controlled cascades. *Lecture Notes in Computer Science*, 950:450–455, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mersenne:1644:CPM

[Mer44] Marin Mersenne. *Cogitata Physica-Mathematica ... [Tractatus de mensuris ponderibus atque nummis ... Hydraulica pneumatica; arsque navigandi. Harmonia theorica, practica.*

Et Mechanica phaenomena. Ballistica et acontismologia]. Antonii Bertier, Paris, France, April 1, 1644. [30], 40 [24], 41–370, [16], 96, [8], 138, [34] + 40 pp. URL `http://www.mersenne.org/prime.htm; http://www.mersenne.org/status.htm`. Three volumes. This is the book that introduced the conjecture that numbers of the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127,$ and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107,$ and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and $61, 89,$ and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing 4,053,946 digits.

Merkle:1978:SCI

[Mer78] Ralph C. Merkle. Secure communications over insecure channels. *Communications of the Association for Computing Machinery*, 21(4):294–299, April 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Merkle:1980:PPK

[Mer80] R. C. Merkle. Protocols for public key cryptosystems. In IEEE [IEE80], page ?? LCCN QA76.9.A25S95 1980.

Merkle:1982:PPK

[Mer82a] Ralph C. Merkle. Protocols for public key cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 73–104. Westview, Boulder, CO, 1982.

Merkle:1982:SAP

[Mer82b] Ralph C. (Ralph Charles) Merkle. *Secrecy, authentication, and public key systems*, volume 18 of *Computer science. Systems programming*. UMI Research Press, Ann Arbor, MI, USA, 1982. ISBN 0-8357-1384-9. 104 pp. LCCN QA76.9.A25 M47 1982. Revision of the author's thesis (Ph.D.—Stanford University, 1979).

Merkle:1988:DSB

[Mer88] Ralph C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, *Advances in Cryptology — CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. ISBN 3-540-48184-2.

Merkle:1989:CDS

[Mer89] Ralph C. Merkle. A certified digital signature. *Lecture Notes in Computer Science*, 435:218–238, 1989. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `https://link.springer.com/chapter/10.1007/0-387-34805-0_21`.

Merkle:1990:OWH

[Mer90a] R. Merkle. One way hash functions and DES. In Brassard [Bra90c], pages 428–446 (or 428–466??). CODEN LNCSD9. ISBN 0-387-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435`. Based on unpublished paper from 1979 and his Ph.D thesis, Stanford, 1979.

Merkle:1990:CDS

[Mer90b] R. C. Merkle. A certified digital signature (subtitle: That antique paper from 1979). In Brassard [Bra90c], pages 218–238. CODEN LNCSD9. ISBN 0-387-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350218.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0435/04350218.pdf`. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Merkle:1991:FSE

[Mer91] Ralph C. Merkle. Fast software encryption functions. *Lecture Notes in Computer Science*, 537: 476–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370476.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0537/05370476.pdf`.

Mercuri:1993:IRC

[Mer93] Rebecca Mercuri. Inside risks: Corrupted polling. *Communications of the Association for Computing Machinery*, 36(11):122, 94, November 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/163380.html`.

Merrill:1997:ARD

[Mer97] C. R. Merrill. An attorney's roadmap to the digital signature guidelines. *Lecture Notes in Computer Science*, 1318:291–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Meyer:1973:DCC

[Mey73] C. H. Meyer. Design considerations for cryptography. *AFIPS Conference Proceedings*, 42(??):603–606, ???? 1973.

Meyer:1996:RPE

[Mey96a] G. Meyer. RFC 1968: The PPP encryption control protocol (ECP), June 1996. URL `ftp://ftp.internic.net/rfc/rfc1968.txt`; `https://www.math.utah.edu/pub/rfc/rfc1968.txt`. Status: PROPOSED STANDARD.

Meyer:1996:PMT

[Mey96b] Helen Meyer. A proposed mode for triple-DES encryption. *Computers and Security*, 15(4):322, ???? 1996. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404896889668`.

Meyer:1997:YHI

[Mey97a] Carl Meyer. 20 years of DES — how it was designed. *Computers and Security*, 16(6):518, ???? 1997. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S016740489784672X`.

Meyer:1997:UTO

[Mey97b] Carl Meyer. Update on triple DES operations and crypto system initialization. *Computers and Security*, 16(6):518, ???? 1997. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404897846706`.

Meyer:1999:BAB

[Mey99] Helen Meyer. 56-bit DES algorithm broken in record time. *Computers and Security*, 18(2):149–150, ???? 1999. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404899800327`.

McGraw:1997:UKJ

[MF97] Gary McGraw and Edward Felten. Understanding the keys to Java security: the sandbox and authentication. *JavaWorld: IDG's magazine for the Java community*, 2(5):??, May 1997. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/jw-05-1997/jw-05-security.htm`.

Murino:1995:RNU

[MFG95] V. Murino, E. Frumento, and F. Gabino. Restoration of noisy underwater acoustic images using Markov random fields. *Lecture Notes in Computer Science*, 974:355–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mihaljevic:1991:CCP

[MG91] M. J. Mihaljevic and J. D. Golic. A comparison of cryptanalytic principles based on iterative error-correction. *Lecture Notes in Computer Science*, 547: 527–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Madson:1998:RUHa

[MG98a] C. Madson and R. Glenn. RFC 2403: The use of HMAC-MD5-96 within ESP and AH, November 1998. URL `ftp://ftp.internic.net/rfc/rfc2403.txt`; `https://www.math.utah.edu/pub/rfc/rfc2403.txt`. Status: PROPOSED STANDARD.

Madson:1998:RUHb

[MG98b] C. Madson and R. Glenn. RFC 2404: The use of HMAC-SHA-1-96 within ESP and AH, November 1998. URL `ftp://ftp.internic.net/rfc/rfc2404.txt`; `https://www.math.utah.edu/pub/rfc/rfc2404.txt`. Status: PROPOSED STANDARD.

Mackenzie:1998:LPS

[MGL+98] Don Mackenzie, Andrew J. Gryc, Graziano Lo Russo, Gary Clouse, C. J. Hinke, Bruce E. Hogman, Thomas Fleischer, and John Graham-Cumming. Letters: The passport system does work; real-time sound; C++ versus Java; online op-ed; hard encryption; Y2K; VerCheck update. *Dr. Dobb's Journal of Software Tools*, 23(12): 12, 16–17, December 1998. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/`.

Merkle:1978:HIS

[MH78] Ralph Merkle and Martin E. Hellman. Hiding information and signatures in trap door knapsacks. *IEEE Transactions on Information Theory*, 24(5):525–530, 1978. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Merkle:1981:SME

[MH81] Ralph C. Merkle and Martin E. Hellman. On the security of multiple encryption. *Communications of the Association for Computing Machinery*, 24(7): 465–467, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Michels:1996:RDS

[MH96] M. Michels and P. Horster. On the risk of disruption in several multiparty signature schemes. *Lecture Notes in Computer Science*, 1163:334–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

McPherson:1998:CRH

[MHMW98] W. D. McPherson, D. A. Hill, L. Mai, and J. S. Wright. Chip rate hopping provides low probability of detection for direct sequence signals. *Electronics Letters*, 34(7):628–629, April 2, 1998. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072135.html.

Majzik:1996:MCU

[MHPS96] I. Majzik, W. Hohl, A. Pataricza, and V. Sieh. Multiprocessor checking using watchdog processors. *International Journal of Computer Systems Science and Engineering*, 11(5):301–310, September 1996. CODEN CSSEEI. ISSN 0267-6192.

Matsumoto:1988:PQP

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message encryption. In Gunther [Gun88b], pages 419–453. CODEN LNCSD9. ISBN 0-387-50251-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.330; QA76.9.A25 E9641 1988. Sponsored by the International Association for Cryptologic Research.

Matsumoto:1990:EAC

[MI90] Tsutomu Matsumoto and Hideki Imai. An efficient asymmetric cryptosystem supporting authenticity and confidentiality with public multivariate polynomial tuples. *Electronics and communications in Japan. Part 3, Fundamental electronic science*, 73(7):1–17, 1990. CODEN ECJSER. ISSN 1042-0967 (print), 1520-6440 (electronic).

Moulin:1999:ECG

[MI99] B. Moulin and H. Irandoust. Extending the conceptual graph approach to represent evaluative attitudes in discourse. *Lecture Notes in Computer Science*, 1640:140–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Michener:1988:TSK

[Mic88] John R. Michener. A tool for secret key cryptography. *Dr. Dobb's Journal of Software Tools*, 13(8):50–52, 55, 96, August 1988. CODEN DDJOEB. ISSN 0888-3076.

Micali:1993:FPC

[Mic93a] S. Micali. Fair public-key cryptosystems. In Brickell [Bri93], pages 113–138. CODEN LNCSD9. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1992. DM104.00.

Micali:1993:FPK

[Mic93b] Silvio Micali. Fair public-key cryptosystems (rough draft). *Lecture Notes in Computer Science*, 740: 113–138, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0740/07400113.htm; http://link.springer-ny.com/link/service/series/0558/papers/0740/07400113.pdf.

Micciancio:1997:ODS

[Mic97] Daniele Micciancio. Oblivious data structures: applications to cryptography. In ACM [ACM97c], pages 456–464. ISBN 0-89791-888-6. LCCN QA76.5 .A849 1997. URL http://www.acm.org/pubs/articles/proceedings/stoc/258533/p456-micciancio/p456-micciancio.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/258533/p456-micciancio/. ACM order no. 508970.

Mihailescu:1994:FGP

[Mih94] Preda Mihailescu. Fast generation of provable primes using search in arithmetic progressions. In Desmedt [Des94b], pages 282–293. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390282.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390282.pdf.

Mihaljevic:1996:FCS

[Mih96] M. Mihaljevic. A faster cryptanalysis of the self-shrinking generator. *Lecture Notes in Computer Science*, 1172:182–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Millikin:1943:ECCa

[Mil43a] Donald D. Millikin. *Elementary cryptography and cryptanalysis*, volume 56 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1943. ISBN 0-89412-173-1 (soft cover), 0-89412-174-X (library bound). vii + 132 pp. LCCN ????

Millikin:1943:ECCb

[Mil43b] Donald D. Millikin. *Elementary cryptography and cryptanalysis*. New York University Bookstore, New York, NY, USA, second edition, 1943. vii + 132 + 1 + 28 pp.

Millikin:1943:ECCc

[Mil43c] Donald D. Millikin. *Elementary cryptography and cryptanalysis*. Aegean Park Press, Laguna Hills, CA, USA, third edition, 1943. vii + 132 pp.

Miller:1976:RHT

[Mil76] G. L. Miller. Reimann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13:300–317, 1976. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Miller:1985:PES

[Mil85] Jay I. Miller. A private-key encryption system based on plane geometry. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1985. iv + 33 + 115 pp.

Miller:1986:UEC

[Mil86] V. S. Miller. Uses of elliptic curves in cryptography. In Williams [Wil86b], pages 417–426. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm; http://www.springerlink.com/content/978-0-387-16463-2; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=218.

Millen:1987:CCC

[Mil87a] Jonathan K. Millen. Covert channel capacity. In IEEE [IEE87c], pages 60–66. ISBN 0-8186-8771-1 (hardback), 0-8186-0771-8 (paperback), 0-8186-4771-X (microfiche). LCCN QA 76.9 A25 I43 1987. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1016.html`. IEEE catalog number 87CH2416-6. Computer Society Order Number 771.

Mills:1987:RDP

[Mil87b] D. L. Mills. RFC 1004: Distributed-protocol authentication scheme, April 1, 1987. URL `ftp://ftp.internic.net/rfc/rfc1004.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc1004.txt`. Status: EXPERIMENTAL.

Millikin:1992:ECC

[Mil92] Donald D. Millikin. *Elementary cryptography and cryptanalysis*, volume 56 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1992. ISBN 0-89412-173-1 (soft cover), 0-89412-174-X (library bound). vii + 132 pp. LCCN ????

Miller:1995:HWK

[Mil95] David T. (David Thurman) Miller. How will I know you?: Encryption and the development of personal communications privacy in the United States. Thesis (M.A), University of Kentucky, Lexington, Ky., 1995. v + 124 pp.

Millan:1996:LOA

[Mil96a] W. Millan. Low order approximation of cipher functions. *Lecture Notes in Computer Science*, 1029: 144–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Miller:1996:CME

[Mil96b] A. R. Miller. The cryptographic mathematics of Enigma. Technical report, Center for Cryptologic History, National Security Agency, Washington, DC, USA, 1996.

Matsumoto:1993:VIA

[MILY93] T. Matsumoto, H. Imai, C.-S. Laih, and S.-M. Yen. On verifiable implicit asking protocols for RSA computation. *Lecture Notes in Computer Science*, 718: 296–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mintzer:1997:EIDa

[Min97] Fred Mintzer. Effective and ineffective digital watermarks. Research report

RC 20933, IBM T.J. Watson Research Center, Yorktown Heights, NY, USA, July 24, 1997. 4 pp.

Misarsky:1997:MAU

[Mis97] Jean-François Misarsky. A multiplicative attack using LLL algorithm on RSA signatures with redundancy. *Lecture Notes in Computer Science*, 1294: 221–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940221.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940221.pdf`.

Misarsky:1998:HDR

[Mis98] Jean-François Misarsky. How (not) to design RSA signature schemes. *Lecture Notes in Computer Science*, 1431:14–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310014.htm; http://link.springer-ny.com/link/service/series/0558/papers/1431/14310014.pdf`.

Mitchell:1976:EAD

[Mit76] James Melvin Mitchell. Encryption algorithm for data security based on a polyalphabetic substitution scheme and a pseudorandom number generator. Thesis (M.S.), University of Tennessee, Knoxville, Knoxville, TN, USA, 1976. v + 83 pp.

Mitchell:1989:MDS

[Mit89] C. Mitchell. Multi-destination secure electronic mail. *The Computer Journal*, 32(1):13–15, February 1989. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/32/1/13.full.pdf+html; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_01/tiff/13.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_01/tiff/14.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_01/tiff/15.tif`.

Mitchell:1992:AMI

[Mit92a] C. J. Mitchell. Authenticating multicast Internet electronic mail messages using a bidirectional MAC is insecure. *IEEE Transactions on Computers*, 41 (4):505–507, April 1992. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=135563.

Mitchell:1992:CCI

[Mit92b] Chris Mitchell. *Cryptography and coding II*. The Institute of Mathematics and Its Applications conference series; new ser., 33. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1992. ISBN 0-19-853393-4. xi + 301 pp. LCCN QA268.C75 1992. UK£40.00, US$60.00. Based on the proceedings of a conference organized by the Institute of Mathematics and its Applications on cryptography and coding, held at the Royal Agricultural College, Cirencester, in December 1989.

Miyaguchi:1990:FCC

[Miy90] Shoji Miyaguchi. The FEAL-8 cryptosystem and a call for attack. *Lecture Notes in Computer Science*, 435:624–627, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Miyaguchi:1991:FCF

[Miy91] S. Miyaguchi. The FEAL cipher family. *Lecture Notes in Computer Science*, 537: 627–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Miyaji:1993:ECS

[Miy93a] Atsuko Miyaji. Elliptic curves over $\mathbf{F}_p$ suitable for cryptosystems. *Lecture Notes in Computer Science*, 718:479–491, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Miyaji:1993:OEC

[Miy93b] Atsuko Miyaji. On ordinary elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 739: 460–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Miyano:1993:MEN

[Miy93c] Hiroshi Miyano. A method to estimate the number of ciphertext pairs for differential cryptanalysis. *Lecture Notes in Computer Science*, 739:51–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Miyaji:1996:MRS

[Miy96] A. Miyaji. A message recovery signature scheme equivalent to DSA over elliptic curves. *Lecture Notes in Computer Science*, 1163:1–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Miyaji:1999:ECC

[Miy99] Atsuko Miyaji. Elliptic curve cryptosystems. *Sūrikaisekikenkyūsho Kōkyūroku*, 1098:138–146, 1999. Applied mathematics of discrete integrable systems (Kyoto, 1998).

Mjolsnes:1993:PCP

[Mjo93] Stig Fr. Mjolsnes. Privacy, cryptographic pseudonyms, and the state of health. *Lecture Notes in Computer Science*, 739:493–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Morii:1992:PSP

[MK92] Masakatu Morii and Masao Kasahara. Perfect staircase profile of linear complexity for finite sequences. *Information Processing Letters*, 44(2):85–89, November 19, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Moskowitz:1994:CCH

[MK94] I. S. Moskowitz and M. H. Kang. Covert channels — here to stay. In IEEE [IEE94b], pages 235–243. ISBN 0-7803-1856-0 (casebound), 0-7803-1855-2 (softbound), 0-7803-1857-9 (microfiche). LCCN QA 76.76 R44 C668 1994. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/034217.html`. IEEE catalog number 94CH3415-7.

Mazieres:1999:SKM

[MKKW99] David Mazières, Michael Kaminsky, M. Frans Kaashoek, and Emmett Witchel. Separating key management from file system security. *Operating Systems Review*, 33(5):124–139, December 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Maibaum:1999:SRS

[MKL99] T. S. E. Maibaum, P. Kan, and K. Lano. Systematising reactive system design. *Lecture Notes in Computer Science*, 1548:17–22, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Miyazaki:1999:TFI

[MKS99] Shingo Miyazaki, Ikuko Kuroda, and Kouichi Sakurai. Toward fair international key escrow — an attempt by distributed trusted third agencies with threshold cryptography. *Lecture Notes in Computer Science*, 1560: 171–187, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/`

link/service/series/0558/bibs/1560/15600171.htm; http://link.springer-ny.com/link/service/series/0558/papers/1560/15600171.pdf.

Monge:1967:NMC

[ML67] Alf Monge and O. G. Landsverk. *Norse medieval cryptography in runic carvings*. Norseman Press, Glendale, CA, USA, 1967. 224 pp. LCCN E105 .M65. Includes bibliographies.

Maulucci:1987:HAC

[ML87] Ruth A. Maulucci and J. A. N. Lee. Happenings: The 25th Anniversary of Committee X3; The Code-Breaking Computers of 1944. *Annals of the History of Computing*, 9(3/4):345–356, July/September 1987. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1987/pdf/a3345.pdf; http://www.computer.org/annals/an1987/a3345abs.htm.

Mao:1998:CPO

[ML98] Wenbo Mao and Chae Hoon Lim. Cryptanalysis in prime order subgroups of Z_n^*. *Lecture Notes in Computer Science*, 1514:214–226, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Matyas:1991:KSB

[MLA91] S. M. Matyas, A. V. Le, and D. G. Abraham. A key-management scheme based on control vectors. *IBM Systems Journal*, 30(2):175–191, 1991. CODEN IBMSA7. ISSN 0018-8670.

Muffett:1995:BPK

[MLLG95] A. Muffett, P. Leyland, A. Lenstra, and J. Gillogly. The BlackNet 384-bit PGP key has been BROKEN. Message posted to sci.crypt and other newsgroups on June 26, 1995., June 26, 1995.

Matyas:1978:GDI

[MM78] Stephen M. Matyas and Carl H. Meyer. Generation, distribution, and installation of cryptographic keys. *IBM Systems Journal*, 17(2):126–137, 1978. CODEN IBMSA7. ISSN 0018-8670.

Meyer:1982:CND

[MM82] Carl H. Meyer and Stephen M. Matyas. *Cryptography: a new dimension in computer data security: a guide for the design and implementation of secure systems*. John Wiley and Sons, Inc., New York, NY, USA, 1982. ISBN 0-471-04892-5. xxi + 755 pp. LCCN Z103 .M55. US$39.95.

Moler:1983:SVA

[MM83] Cleve Moler and Donald Morrison. Singular value analysis of cryptograms. *American Mathematical Monthly*, 90(2):78–87, February 1983. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Meadows:1987:MSA

[MM87] C. Meadows and D. Mutchler. Matching secrets in the absence of a continuously available trusted authority. *IEEE Transactions on Software Engineering*, SE-13(2):289–292, February 1987. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702207.

Magliveras:1990:LCP

[MM90a] Spyros S. Magliveras and Nasir D. Memon. The linear complexity profile of cryptosystem PGM. *Congressus Numerantium*, 72:51–60, 1990. ISSN 0384-9864.

Magliveras:1990:PCP

[MM90b] Spyros S. Magliveras and Nasir D. Memon. Properties of cryptosystem PGM. *Lecture Notes in Computer Science*, 435:447–460, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Moskovitz:1992:CCC

[MM92a] I. S. Moskovitz and A. R. Miller. The channel capacity of a certain noisy timing channel. *IEEE Transactions on Information Theory*, IT-38(4):1339–1343, ???? 1992. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/021229.html.

Moskowitz:1992:IDI

[MM92b] I. S. Moskowitz and A. R. Miller. The influence of delay on an idealized channel's bandwidth. In IEEE [IEE92c], pages 63–67. ISBN 0-8186-2825-1 (paperback) 0-8186-2826-X (microfiche) 0-8186-2827-8 (casebound). LCCN QA 76.9 A25 I34 1992. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1017.html. IEEE Catalog Number 92CH3157-5. IEEE Computer Society Press order number 2825.

Moskowitz:1994:STC

[MM94] I. S. Moskowitz and A. R. Miller. Simple timing channels. In IEEE [IEE94d], pages 56–64. ISBN 0-8186-5675-1 (paperback), 0-8186-

5676-X (microfiche) 0-8186-5677-8 (case). LCCN QA 76.9 A25 I34 1994. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/032819.html. IEEE Catalog Number 94CH3444-7.

Moldovyan:1995:FSE

[MM95] A. Moldovyan and N. Moldovyan. Fast sofware encryption system based on local pseudorandomness. *Comput. Sci. J. Moldova*, 3(3):252–262, 1995. ISSN 1561-4042.

Meadows:1996:CCC

[MM96a] C. Meadows and I. Moskowitz. Covert channels — a context-based view. In Anderson [And96c], pages 73–93. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054230.html.

Meyer:1996:PKC

[MM96b] Bernd Meyer and Volker Müller. A public key cryptosystem based on elliptic curves over $\mathbf{Z}/n\mathbf{Z}$ equivalent to factoring. *Lecture Notes in Computer Science*, 1070:49–59, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700049.htm; http://link.springer-ny.com/link/service/series/0558/papers/1070/10700049.pdf.

Mueller:1998:SPK

[MM98a] S. Mueller and W. B. Mueller. The security of public key cryptosystems based on integer factorization. *Lecture Notes in Computer Science*, 1438:9–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Muller:1998:SPK

[MM98b] Siguna Müller and Winfried B. Müller. The security of public key cryptosystems based on integer factorization. *Lecture Notes in Computer Science*, 1438:9–23, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1438/14380009.htm; http://link.springer-ny.com/link/service/series/0558/papers/1438/14380009.pdf.

Marchignoli:1999:AVC

[MM99a] D. Marchignoli and F. Martinelli. Automatic verification of cryptographic protocols through compositional analysis techniques. *Lecture Notes in Computer Sci-*

ence, 1579:148–162, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Meddes:1999:ABV

[MM99b] J. Meddes and E. McKenzie. An agent-based visualisation architecture. *Lecture Notes in Computer Science*, 1614:43–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mirza:1999:OKS

[MM99c] F. Mirza and S. Murphy. An observation on the key schedule of Twofish. In ????, editor, *Second AES Candidate Conference Proceedings*, page ?? ????, ????, March 1999. ISBN ???? LCCN ????

Moldovyan:1997:SEN

[MMI97] A. Moldovyan, N. Moldovyan, and V. Izbash. Software encryption: new 64-bit block cryptoscheme. *Comput. Sci. J. Moldova*, 5(1):10–19, 1997. ISSN 1561-4042.

MattosBrasil:1998:CCC

[MMM+98] L. Mattos Brasil, F. Mendes De Azevedo, Muniz, J. Barreto, and M. Noirhomme-Fraiture. Complexity and cognitive computing. *Lecture Notes in Computer Science*, 1415:408–417, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Matheson:1998:RSD

[MMST98] L. R. Matheson, S. G. Mitchell, T. G. Shamoon, and R. E. Tarjan. Robustness and security of digital watermarks. *Lecture Notes in Computer Science*, 1465:227–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Magliveras:1990:CTC

[MMT90] Spyros S. Magliveras, Nasir D. Memon, and Kok C. Tam. Complexity tests of cryptosystem PGM. *Congressus Numerantium*, 79:61–68, 1990. ISSN 0384-9864.

Muller:1981:SRP

[MN81] Winfried B. Müller and Wilfried Nöbauer. Some remarks on public-key cryptosystems. *Studia Sci. Math. Hungar.*, 16(1-2): 71–76, 1981. CODEN SSMHAX. ISSN 0081-6906.

Muller:1986:CDS

[MN86] Winfried B. Müller and Rupert Nöbauer. Cryptanalysis of the Dickson-scheme. *Lecture Notes in Computer Science*, 219:50–61, 1986. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

MRaihi:1997:XFO

[MNSV97] David M'Raïhi, David Naccache, Jacques Stern, and

Serge Vaudenay. XMX: a firmware-oriented block cipher based on modular multiplications. *Lecture Notes in Computer Science*, 1267:166–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670166.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670166.pdf`.

Moulin:1999:ITA

[MO99] Pierre Moulin and Joseph O'Sullivan. Information-theoretic analysis of information hiding. *IEEE Transactions on Information Theory*, 49(3):563–593, March 1999. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.2370`.

Mock:1997:BDS

[Moc97] Kevin Gary Mock. Behavioral description and simulation of an International Data Encryption Algorithm chip. Thesis (M.S.), North Carolina State University, Raleigh, NC, USA, 1997. vi + 85 pp.

Mohtashemi:1992:CHC

[Moh92] Mojdeh Mohtashemi. On the cryptanalysis of Huffman codes. Thesis (M.S.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, May 1992. 35 pp. Also published as Technical report MIT/LCS/TR-617.

Matsumoto:1982:DTL

[MOI82] Tsutomu Matsumoto, Tomoko Okada, and Hideki Imai. Directly transformed link encryption. *Systems-Comput.-Controls*, 13(6): 36–44 (1983), 1982. CODEN SYCCBB. ISSN 0096-8765.

Mok:1997:KNF

[Mok97] Wai Yin Mok. On keys and normal forms. *Information Processing Letters*, 62 (5):255–258, July 2, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Moldovyan:1998:NEP

[Mol98] N. A. Moldovyan. Nondeterministic encryption with provable nonequivalence of all modifications of a cryptographic algorithm. *Kibernet. Sistem. Anal.*, 5:61–68, 188, 1998. ISSN 0023-1274.

Morita:1991:SCT

[MOM91] Hikaru Morita, Kazuo Ohta, and Shoji Miyaguchi. A switching closure test to analyze cryptosystems (extended abstract). *Lecture Notes in Computer Science*, 576:183–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760183.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760183.pdf.

Montgomery:1985:MMT

[Mon85] Peter L. Montgomery. Modular multiplication without trial division. *Mathematics of Computation*, 44 (170):519–521, April 1985. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journals/mcom/1985-44-170/S0025-5718-1985-0777282-X/.

Monagan:1993:GPD

[Mon93] M. Monagan. Gauss: a parameterized domain of computation system with support for signature functions. *Lecture Notes in Computer Science*, 722:81–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Montagu:1996:MWN

[Mon96] Ewen Montagu. *The man who never was: World War II's boldest counterintelligence operation*. Bluejacket books. Naval Institute Press, Annapolis, MD, USA, 1996. ISBN 1-55750-448-2 (paperback). 160 + 8 pp. LCCN D810.S8 M6 2001. CIP rev.

Moore:1992:PFC

[Moo92] J. H. Moore. Protocol failures in cryptosystems. In *Contemporary cryptology*, pages 541–558. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992.

Morland:1666:NMC

[Mor66] Sir Samuel Morland. *A New Method of Cryptography*. ????, ????, 1666. 12 pp. Microfilm in Folger Shakespeare Library, Washington, DC, USA.

Morrice:1692:EB

[Mor92] Roger Morrice. *Entring Book*. ????, ????, 1692. 1500 pp. URL http://www.hist.cam.ac.uk/seminars_events/events/roger-morrice.html; http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2003/08/29/ndiary29.xml. Three volumes.

Morrison:1983:SEA

[Mor83] D. R. Morrison. Subtractive encryptors: alternatives to the DES. *ACM*

SIGACT News, 15(1):67–77, Winter–Spring 1983. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Morain:1988:IGP

[Mor88] F. Morain. Implementation of the Goldwasser-Killian-Atkin primality testing algorithm. Technical report, Institut de la Recherche en Informatique et Automatique, now Institut National de Recherche en Informatique et Automatique (INRIA), Domaine de Voluceau, Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex, France, 1988. ?? pp. Project ALGO, INRIA.

Mora:1989:AAA

[Mor89] Teo Mora, editor. *Applied algebra, algebraic algorithms, and error-correcting codes: 6th international conference, AAECC-6, Rome, Italy, July 4–8, 1988: proceedings*, volume 357 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989. CODEN LNCSD9. ISBN 0-387-51083-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .A35 1988. US$36.00 (USA).

Morris:1992:FMC

[Mor92] Stephen Brent Morris. *The Folger manuscript: the cryptanalysis and interpretation of an American Masonic manuscript*, volume 23 of *Publications of the Masonic Book Club*. Masonic Book Club, Bloomington, IL, USA, 1992. xxxii + 255 pp.

Morgan:1997:PAM

[Mor97] Andrew G. Morgan. Pluggable authentication modules for Linux. *Linux Journal*, 44:??, December 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL `ftp://ftp.ssc.com/pub/lj/listings/issue44/2120.tgz`.

MorenoDiaz:1998:NCC

[Mor98] R. Moreno Diaz. Neurocybernetics, codes and computation. *Lecture Notes in Computer Science*, 1416: 1–14, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Moskowitz:1998:C

[Mos98] Scott Moskowitz. So this is convergence? technical, economic, legal, cryptographic, and philosophical considerations for secure implementations of digital watermarking. Technical report, Blue Spike, Inc., Miami, FL, USA (??), March 1998. 96 pp. URL http://www.bluespike.com/papers/convergence.pdf.

Mosses:1999:CGT

[Mos99] P. D. Mosses. CASL: a guided tour of its design. *Lecture Notes in Computer Science*, 1589: 216–240, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Moura:1999:PAP

[Mou99] L. Moura. A polyhedral algorithm for packings and designs. *Lecture Notes in Computer Science*, 1643: 462–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mullin:1988:ONB

[MOVW89] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson. Optimal normal bases in GF(p^n). *Discrete Applied Mathematics*, 22(2):149–161, 1988–1989. CODEN DAMADU. ISSN 0166-218X.

Moynihan:1998:SAE

[Moy98] Daniel P. (Daniel Patrick) Moynihan. *Secrecy: the American experience*. Yale University Press, New Haven, CT, USA, 1998. ISBN 0-300-07756-4. ix + 262 pp. LCCN JK468.S4 M68 1998. Introduction by Richard Gid Powers.

Mevis:1986:SCP

[MP86] Howard Mevis and Janet Plant. *Satellite communications: a practical guide to satellite TV encryption with tips on installing decoders, solving reception problems, and upgrading TVROs*. American Hospital Association, Media Center, Chicago, IL, USA, 1986. 25 pp.

McInnes:1991:IPK

[MP91] J. L. McInnes and B. Pinkas. On the impossibility of private key cryptography with weakly random keys. *Lecture Notes in Computer Science*, 537:421–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Milidiu:1999:EIW

[MPL99] R. L. Milidiu, A. A. Pessoa, and E. S. Laber. Efficient implementation of the WARM-UP algorithm for the construction of length-restricted prefix codes. *Lecture Notes in Computer Science*, 1619:1–17, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mayerwieser:1995:THS

[MPPS95] Wolfgang Mayerwieser, Karl C. Posch, Reinhard Posch, and Volker Schindler. Testing a high-speed data: Path the design of the RSAb crypto chip. *J.UCS: Journal of Universal Computer Science*, 1(11):728–??, November 28, 1995. ISSN 0948-6968. URL http://www.iicm.edu/jucs_1_11/testing_a_high_speed.

Moller:1994:RSW

[MPS94] Steffen Moller, Andreas Pfitzmann, and Ingo Stierand. Rechnergestützte Steganographie: Wie sie Funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist. *Datenschutz und Datensicherheit*, 18(6):318–326, ???? 1994. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/042160.html.

Mori:2002:CSD

[MPS02] G. Mori, F. Paterno, and C. Santoro. CTTE: support for developing and analyzing task models for interactive system design. *IEEE Transactions on Software Engineering*, 28(8):797–813, August 2002. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1027801.

Morillo:1999:WTS

[MPSV99] P. Morillo, C. Padró, G. Sáez, and J. L. Villar. Weighted threshold secret sharing schemes. *Information Processing Letters*, 70(5):211–216, June 21, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.elsevier.nl/gej-ng/10/23/20/48/21/24/abstract.html; http://www.elsevier.nl/gej-ng/10/23/20/48/21/24/article.pdf.

Malek:1995:DCB

[MR95a] M. Malek and V. Rialle. Design of a case-based reasoning system applied to neuropathy diagnosis. *Lecture Notes in Computer Science*, 984:255–265, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Myers:1995:RCM

[MR95b] J. Myers and M. Rose. RFC 1864: The content-MD5 header field, October 1995. URL ftp://ftp.internic.net/rfc/rfc1544.txt; ftp://ftp.internic.net/rfc/rfc1864.txt; https://www.math.utah.edu/pub/rfc/rfc1544.txt; https://www.math.utah.edu/pub/rfc/rfc1864.txt. Obsoletes RFC1544 [Ros93]. Status: DRAFT STANDARD.

McLeod:1998:TMP

[MR98] Jeanette McLeod and Greg

Rose. Torn money and the PGP web of trust. *;login: the USENIX Association newsletter*, 23(7):??, December 1998. CODEN LOGNEM. ISSN 1044-6397. URL `http://www.usenix.org/publications/login/1998-12/tornmoney.html`.

Mrakovcic:1995:EIN

[Mra95] Darko Mrakovcic. *On encryption of infinitesimal neighborhoods in geometric invariants of the conic structure on the space of nearby submanifolds*. Thesis (Ph.D.), State University of New York at Stony Brook, Stony Brook, NY, USA, 1995. x + 213 pp.

Micali:1987:NSP

[MRS87] Silvio Micali, Charles Rackoff, and Bob Sloan. The notion of security for probabilistic cryptosystems (extended abstract). *Lecture Notes in Computer Science*, 263:381–392, 1987. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Micali:1988:NSP

[MRS88] Silvio Micali, Charles Rackoff, and Bob Sloan. The notion of security for probabilistic cryptosystems. *SIAM Journal on Computing*, 17(2):412–426, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Maitra:1999:COA

[MRS99] S. Maitra, B. K. Roy, and P. Sarkar. Ciphertext only attack on LFSR based encryption scheme. *Calcutta Statist. Assoc. Bull.*, 49(195-196):239–254, 1999. CODEN CSTBAA. ISSN 0008-0683.

Mitchell:1989:RHF

[MRW89] Chris Mitchell, Dave Rush, and Michael Walker. A remark on hash functions for message authentication. *Computers and Security*, 8 (1):55–58, February 1, 1989. CODEN CPSEDU. ISSN 0167-4048.

Macalister:1976:SLI

[MS76] Robert Alexander Stewart Macalister and John Sampson. *The secret languages of Ireland: Ogham, Hisperic, Bearlagair na Saer, Bog-Latin, and cryptography, with special reference to the origin and nature of the Shelta language; partly based upon collections and manuscripts of the late John Sampson; with an English-jargon vocabulary*. APA-Philo Press, Amsterdam, The Netherlands, 1976. ISBN 90-6022-276-8. x + 284 pp. LCCN PM9001 .M2 1976. Reprint of the 1937 ed. published by the Cambridge University Press, Cambridge, England.

McEliece:1981:SSR

[MS81] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed–Solomon codes. *Communications of the Association for Computing Machinery*, 24(9): 583–584, September 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Muller-Schloer:1983:MBC

[MS83] C. Müller-Schloer. A microprocessor-based cryptoprocessor. *IEEE Micro*, 3(5):5–15, September/ October 1983. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Moore:1987:CSK

[MS87] J. H. Moore and G. J. Simmons. Cycle structure of the DES for keys having palindromic (or antipalindromic) sequences of round keys. *IEEE Transactions on Software Engineering*, SE-13(2):262–273, February 1987. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702205`.

Meier:1990:NCC

[MS90a] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. *Lecture Notes in Computer Science*, 434: 549–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340549.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340549.pdf`.

Montgomery:1990:FEP

[MS90b] P. L. Montgomery and R. D. Silverman. An FFT extension to the P-1 factoring algorithm. *Mathematics of Computation*, 54: 839–854, 1990. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Meier:1991:CPC

[MS91] Willi Meier and Othmar Staffelbach. Correlation properties of combiners with memory in stream ciphers (extended abstract). *Lecture Notes in Computer Science*, 473: 204–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/`

bibs/0473/04730204.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730204.pdf.

Meier:1993:EMC

[MS93] W. Meier and O. Staffelbach. Efficient multiplication on certain nonsupersingular elliptic curves. *Lecture Notes in Computer Science*, 740:333–344, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Massey:1994:FTA

[MS94] James L. Massey and Shirlei Serconek. A Fourier transform approach to the linear complexity of nonlinearly filtered sequences. In Desmedt [Des94b], pages 332–340. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390332.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390332.pdf.

Meier:1995:SG

[MS95a] W. Meier and O. Staffelbach. The self-shrinking generator. *Lecture Notes in Computer Science*, 950:205–214, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Meier:1995:SSG

[MS95b] Willi Meier and Othmar Staffelbach. The self-shrinking generator. *Lecture Notes in Computer Science*, 950:205–214, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500205.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500205.pdf.

Metzger:1995:RIAa

[MS95c] P. Metzger and W. Simpson. RFC 1828: IP authentication using keyed MD5, August 1995. URL ftp://ftp.internic.net/rfc/rfc1828.txt; https://www.math.utah.edu/pub/rfc/rfc1828.txt. Status: PROPOSED STANDARD.

Metzger:1995:RIAb

[MS95d] P. Metzger and W. Simpson. RFC 1852: IP authentication using keyed SHA, September 1995. URL ftp://ftp.internic.net/rfc/rfc1852.txt; https://www.math.utah.edu/pub/rfc/rfc1852.txt. Status: EXPERIMENTAL.

RFC1852

[MS95e] P. Metzger and W. Simpson. RFC 1852: IP authentication using keyed SHA, September 1995. URL ftp://ftp.internic.net/rfc/rfc1852.txt; https://www.math.utah.edu/pub/rfc/rfc1852.txt. Status: EXPERIMENTAL.

Micali:1995:SMG

[MS95f] Silvio Micali and Ray Sidney. A simple method for generating and sharing pseudo-random functions, with applications to Clipper-like key escrow systems. *Lecture Notes in Computer Science*, 963: 185–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630185.htm; http://link.springer-ny.com/link/service/series/0558/papers/0963/09630185.pdf.

Mambo:1998:NCB

[MS98a] M. Mambo and H. Shizuya. A note on the complexity of breaking Okamoto-Tanaka ID-based key exchange scheme. *Lecture Notes in Computer Science*, 1431:258–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Michels:1998:GCS

[MS98b] M. Michels and M. Stadler. Generic constructions for secure and efficient confirmer signature schemes. *Lecture Notes in Computer Science*, 1403:406–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

MacKenzie:1999:AIH

[MS99a] P. MacKenzie and J. Sorensen. Anonymous investing: Hiding the identities of stockholders. In Franklin [Fra99], pages 212–229. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Maitra:1999:HNR

[MS99b] S. Maitra and P. Sarkar. Highly nonlinear resilient functions optimizing Siegenthaler's inequality. In Wiener [Wie99], pages 198–215. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Miyazaki:1999:KGD

[MS99c] Shingo Miyazaki and Kouichi Sakurai. Key generation and decryption algorithms for distributed RSA cryptosystems. *Sūrikaisekikenkyūsho Kōkyūroku*, 1093(1093): 156–161, 1999. Models of computation and algorithms (Japanese) (Kyoto, 1999).

McLeod:1990:VLD

[MSDS90] Dennis McLeod, Ron Sacks-Davis, and H.-J Schek, editors. *Very large data bases: 16th International Conference on Very Large Data Bases; August 13–16, 1990, Brisbane, Australia*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 1990. ISBN 1-55860-149-X. LCCN QA76.9.D3I559 1990.

Miksch:1999:ASQ

[MSHP99] S. Miksch, A. Seyfang, W. Horn, and C. Popow. Abstracting steady qualitative descriptions over time from noisy, high-frequency data. *Lecture Notes in Computer Science*, 1620: 281–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Moriai:1998:HOD

[MSK98] S. Moriai, T. Shimoyama, and T. Kaneko. Higher order differential attack of a CAST cipher. *Lecture Notes in Computer Science*, 1372:17–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

McClure:1999:HEN

[MSK99a] Stuart McClure, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions*. Osborne/McGraw-Hill, Berkeley, CA, USA, 1999. ISBN 0-07-212127-0. 484 pp. LCCN TK5105.59 .M33 1999. US$39.99.

Moriai:1999:IAB

[MSK99b] S. Moriai, T. Shimoyama, and T. Kaneko. Interpolation attacks of the block cipher: SNAKE. In Knudsen [Knu99c], pages 275–289. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Martin:1997:MAS

[MSN97] K. M. Martin and R. Safavi-Naini. Multisender authentication systems with unconditional security. *Lecture Notes in Computer Science*, 1334:130–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mizuki:1998:ESK

[MSN98] T. Mizuki, H. Shizuya, and T. Nishizeki. Eulerian secret key exchange. *Lecture Notes in Computer Science*, 1449:349–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mizuki:1999:DNS

[MSN99] Takaaki Mizuki, Hiroki Shizuya, and Takao Nishizeki. Dealing necessary and sufficient numbers of cards for sharing a one-bit secret key. *Lecture Notes in Computer Science*, 1592: 389–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920389.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1592/15920389.pdf`.

Martin:1999:BTE

[MSNW99] Keith M. Martin, Rei Safavi-Naini, and Huaxiong Wang. Bounds and techniques for efficient redistribution of secret shares to new access structures. *The Computer Journal*, 42 (8):638–649, ???? 1999. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_42/Issue_08/420638.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_42/Issue_08/pdf/420638.pdf`.

Mambo:1996:HUT

[MSO96] M. Mambo, K. Sakurai, and E. Okamoto. How to utilize the transformability of digital signatures for solving the Oracle Problem. *Lecture Notes in Computer Science*, 1163:322–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Madonia:1993:GSP

[MSS93] M. Madonia, S. Salemi, and T. Sportelli. A generalization of Sardinas and Patterson's algorithm to z-codes. *Theoretical Computer Science*, 108(2):251–270, February 15, 1993. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Michels:1998:SSV

[MSS98] M. Michels, M. Stadler, and H.-M. Sun. On the security of some variants of the RSA signature scheme. *Lecture Notes in Computer Science*, 1485:85–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Meyer:1972:PCC

[MT72] C. H. Meyer and W. L. Tuchman. Pseudorandom codes can be cracked. *Electronic Design*, 20(23):74–76, November 9, 1972. CODEN ELODAW. ISSN 0013-4872 (print), 1944-9550 (electronic).

Mullender:1986:DCD

[MT86] S. J. Mullender and A. S. Tanenbaum. The design of a capability-based distributed operating system. *The Computer Journal*, 29

(4):289–299, August 1986. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/289.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/290.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/291.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/292.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/293.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/294.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/295.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/296.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/297.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/298.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_04/tiff/299.tif.

Matsui:1994:VSH

[MT94] K. Matsui and K. Tanaka. Video-steganography: How to secretly embed a signature in a picture. *IMA Intellectual Property Project proceedings: the journal of the Interactive Multimedia Association Intellectual Property Project*, 1(1):187–205, January 1994. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/043140.html.

Massey:1995:MCM

[MT95] B. C. Massey and E. Tick. Modes of comprehension: Mode analysis of arrays and array comprehensions. *Lecture Notes in Computer Science*, 982:207–222, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Molva:1998:SSA

[MT98] R. Molva and G. Tsudik. Secret sets and applications. *Information Processing Letters*, 65(1):47–55, January 15, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Matsui:1999:CRV

[MT99a] M. Matsui and T. Tokita. Cryptanalysis of a reduced version of the block cipher E2. In Knudsen [Knu99c], pages 71–80. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Melkonian:1999:AAD

[MT99b] V. Melkonian and E. Tardos. Approximation algorithms for a directed network design problem. *Lecture Notes in Computer Science*, 1610:345–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mister:1999:CRL

[MT99c] S. Mister and S. E. Tavares. Cryptanalysis of RC4-like ciphers. *Lecture Notes in Computer Science*, 1556: 131–143, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Marayati:1987:AWA

[MTA87] Muhammad Marayati, Muhammad Hassan Tayyan, and Yahya Mir 'Alam. *'Ilm al-ta'miyah wa-istikhraj al-mu'amma 'inda al-'Arab*. Majma' al-Lughah al-'Arabiyah bi-Dimashq, Damascus, Syria, 1987. various pp. LCCN Z103.4.A65 M37 1987. Abstract in English. Title on added t.p.: Origins of Arab cryptography and cryptanalysis. Contents: al-juz' 1. Dirasat wa-tahqiq li-rasa'il al-Kindi wa-Ibn 'Adlan wa-Ibn al-Durayhim.

Moggi:1999:IMS

[MTES99] E. Moggi, W. Taha, Z. El-Abidine Benaissa, and T. Sheard. An idealized MetaML: Simpler, and more expressive. *Lecture Notes in Computer Science*, 1576:193–207, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mackinnon:1985:OAA

[MTMA85] S. J. Mackinnon, P. D. Taylor, H. Meijer, and S. G. Akl. An optimal algorithm for assigning cryptographic keys to control access in a hierarchy. *IEEE Transactions on Computers*, C-34(9): 797–802, September 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1676635`.

Moriya:1997:DWS

[MTNI97] Takehiro Moriya, Youichi Takashima, Takao Nakamura, and Naoki Iwakami. Digital watermarking schemes based on vector quantization. In IEEE [IEE97e], pages 95–96. ISBN 0-7803-4073-6 (softbound), 0-7803-4074-4 (microfiche). LCCN TK7882.S65I43 1997. IEEE catalog number 97TH8295.

Molva:1992:KAK

[MTVZ92] Refik Molva, Gene Tsudik, Els Van Herreweghen, and Stefano Zatti. KryptoKnight authentication and key distribution system. *Lecture Notes in Computer Science*, 648:155–??, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mu:1992:ICS

[Mu92] Hao Mu. ID-based cryptographic schemes for user identification, key distribution, and digital signature. Thesis (M.S.), Computer Science Telecommunication Program. University of Missouri-Kansas City, Kansas City, MO, USA, 1992. ix + 54 pp.

Mueller:1999:SRB

[Mue99] S. Mueller. On the security of an RSA based encryption scheme. *Lecture Notes in Computer Science*, 1587: 135–148, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Muftic:1988:SMC

[Muf88] Sead Muftic. Security mechanisms for computer networks. current results of the CEC COST-11 ter project. *Computer Networks and ISDN Systems*, 15(1):67–71, 1988. CODEN CNISE9. ISSN 0169-7552.

Muftic:1993:SAO

[Muf93] Sead Muftic, editor. *Security Architecture for Open Distributed Systems*. John Wiley and Sons, Inc., New York, NY, USA, 1993. ISBN 0-471-93472-0. xiii + 281 pp. LCCN QA76.9.A25S376 1993.

Mulherin:1981:FDE

[Mul81] Michael Hugh Mulherin. A file data encryption system using Galois fields. Thesis (M.Sc.Cs.), University of New Brunswick, Ottawa, ON, Canada, 1981. 174 pp. 2 microfiche(s) (174 fr.).

Mullin:1984:NMP

[Mul84] Albert A. Mullin. A note on the mathematics of public-key cryptosystems. *Computers and Security*, 3(1): 45–47, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900269`.

Mulligan:1989:UMA

[Mul89a] Timothy Mulligan, editor. *ULTRA, MAGIC, and the Allies*, volume 1 of *Covert warfare*. Garland, New York, NY, USA, 1989. ISBN 0-8240-7950-7. (various) pp. LCCN D810.S7 C66 1989 vol. 1; D810.C88. US$60.00.

Mullin:1989:LEN

[Mul89b] Albert A. Mullin. Letter to the editor: “The new Mersenne conjecture” [Amer. Math. Monthly **96** (1989), no. 2, 125–128, MR

90c:11009] by P. T. Bateman, J. L. Selfridge and S. S. Wagstaff, Jr. *American Mathematical Monthly*, 96 (6):511, ???? 1989. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). See [BSW89]. Conjectures that "$M_n(= 2^n - 1)$ is the product of two distinct primes only if n is either a prime p or the square of a prime q, in which case precisely one prime factor of M_n is Mersenne, vis. M_q.".

Muller:1999:SRB

[Mül99] Siguna Müller. On the security of an RSA based encryption scheme. *Lecture Notes in Computer Science*, 1587:135–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1587/15870135.htm; http://link.springer-ny.com/link/service/series/0558/papers/1587/15870135.pdf.

Mund:1991:ZCP

[Mun91a] S. Mund. Ziv–Lempel complexity for periodic sequences and its cryptographic application. *Lecture Notes in Computer Science*, 547:114–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mund:1991:ZLC

[Mun91b] Sibylle Mund. Ziv–Lempel complexity for periodic sequences and its cryptographic application. *Lecture Notes in Computer Science*, 547:114–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470114.htm; http://link.springer-ny.com/link/service/series/0558/papers/0547/05470114.pdf.

Muraszko:1987:CVR

[Mur87] J. T. Muraszko, editor. *Colloquium on Vehicle Route Guidance, Navigation and Location Systems (Wednesday, 11 February 1987: London, England)*. IEE, London, UK, 1987. LCCN TE228 .C66 1987. Digest no.: 1987/21.

Murphy:1996:CC

[Mur96] M. Maureen Murphy. *Cyberbanking and cryptography*. Washington, DC, USA, March 12, 1996. 6 pp.

Murphy:1999:OST

[Mur99] Sean Murphy. An observation on the schedule of Twofish. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Musser:1992:UVE

[Mus92] Frederic O. Musser. Ultra vs Enigma: Goucher's top secret contribution to victory in Europe in World War II. *Goucher Quarterly*, 70(2):4–7, ???? 1992. URL http://cdm16235.contentdm.oclc.org/cdm/compoundobject/collection/p16235coll16/id/589/rec/328.

Maruyama:1998:TGH

[MUSM98] O. Maruyama, T. Uchida, T. Shoudai, and S. Miyano. Toward genomic hypothesis creator: View designer for discovery. *Lecture Notes in Computer Science*, 1532: 105–116, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Menezes:1990:IEC

[MV90] Alfred Menezes and Scott Vanstone. The implementation of elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 453:2–13, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Menezes:1991:ACC

[MV91] Alfred J. Menezes and Scott A. Vanstone, editors. *Advances in cryptology — CRYPTO '90: proceedings*, volume 537 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. CODEN LNCSD9. ISBN 0-387-54508-5 (New York), 3-540-54508-5 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1990. Conference held Aug. 11–15, 1990, at the University of California, Santa Barbara.

Meijers:1993:EMV

[Mv93] Joost Meijers and Johan van Tilburg. Extended majority voting and private-key algebraic-code encryptions. *Lecture Notes in Computer Science*, 739: 288–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Menezes:1998:C

[MV98] A. J. Menezes and S. A. Vanstone. Crypto '90. *Lecture Notes in Computer Science*, 1440:119–126, 1998.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mu:1999:DD

[MVN99] Yi Mu, Vijay Varadharajan, and Khan Quac Nguyen. Delegated decryption. *Lecture Notes in Computer Science*, 1746:258–269, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Menezes:1997:HAC

[MVV97] A. J. (Alfred J.) Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1997. ISBN 0-8493-8523-7. xxviii + 780 pp. LCCN QA76.9.A25 M463 1997. URL `http://www.cacr.math.uwaterloo.ca/hac`.

Menezes:1993:CPE

[MVZ93] Alfred J. Menezes, Scott A. Vanstone, and Robert J. Zuccherato. Counting points on elliptic curves over $\mathbf{F}_{2^m}$. *Mathematics of Computation*, 60(201):407–420, January 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Muller:1998:DLB

[MVZ98] Volker Müller, Scott Vanstone, and Robert Zuccherato. Discrete logarithm based cryptosystems in quadratic function fields of characteristic 2. *Designs, Codes, and Cryptography*, 14(2):159–178, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Manber:1994:AAM

[MW94] Udi Manber and Sun Wu. An algorithm for approximate membership checking with application to password security. *Information Processing Letters*, 50 (4):191–197, May 25, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Maurer:1996:TCW

[MW96a] U. Maurer and S. Wolf. Towards characterizing when information-theoretic secret key agreement is possible. *Lecture Notes in Computer Science*, 1163: 196–209, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061811.html`.

Maurer:1996:DO

[MW96b] U. M. Maurer and S. Wolf. Diffie–Hellman oracles. *Lec-*

ture Notes in Computer Science, 1109:268–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Maurer:1996:DHO

[MW96c] Ueli M. Maurer and Stefan Wolf. Diffie–Hellman oracles. *Lecture Notes in Computer Science*, 1109: 268–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090268.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090268.pdf.

Maurer:1997:PAS

[MW97] Ueli M. Maurer and Stefan Wolf. Privacy amplification secure against active adversaries. *Lecture Notes in Computer Science*, 1294:307–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940307.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940307.pdf.

MacNish:1998:BRD

[MW98a] C. K. MacNish and M.-A. Williams. From belief revision to design revision: Applying theory change to changing requirements. *Lecture Notes in Computer Science*, 1359:206–220, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Memon:1998:PDM

[MW98b] N. Memon and P. W. Wong. Protecting digital media content. *Communications of the Association for Computing Machinery*, 41(7): 35–43, July 1998. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073153.html.

Merkle:1998:SSR

[MW98c] J. Merkle and R. Werchner. On the security of server-aided RSA protocols. *Lecture Notes in Computer Science*, 1431:99–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Merkle:1998:SSA

[MW98d] Johannes Merkle and Ralph Werchner. On the security of server-aided RSA protocols. *Lecture Notes in Computer Science*, 1431: 99–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310099.htm; http://link.springer-ny.com/link/service/series/0558/papers/1431/14310099.pdf.

Maurer:1999:RBB

[MW99] Ueli M. Maurer and Stefan Wolf. The relationship between breaking the Diffie–Hellman protocol and computing discrete logarithms. *SIAM Journal on Computing*, 28(5):1689–1721, October 1999. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/30274.

Malkin:1999:ESG

[MWB99] M. Malkin, T. Wu, and D. Boneh. Experimenting with shared generation of RSA keys. In *Internet Society's 1999 Symposium on Network and Distributed System Security (SNDSS)*, pages 43–56. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1999. ISBN ???? LCCN ???? URL http://theory.stanford.edu/~dabo/papers/ShareExp.ps.

Mitchell:1994:CPA

[MWW94] Chris Mitchell, Michael Walker, and Peter Wild. The combinatorics of perfect authentication schemes. *SIAM Journal on Discrete Mathematics*, 7(1):102–107, February 1994. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Maurer:1991:NIP

[MY91] Ueli M. Maurer and Yacov Yacobi. Non-interactive public-key cryptography. *Lecture Notes in Computer Science*, 547:498–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470498.htm; http://link.springer-ny.com/link/service/series/0558/papers/0547/05470498.pdf.

Matsui:1993:NMK

[MY93a] M. Matsui and A. Yamagishi. A new method for known plaintext attack of FEAL cipher. *Lecture Notes in Computer Science*, 658:81–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Maurer:1993:RNI

[MY93b] Ueli M. Maurer and Yacov Yacobi. A remark on a non-interactive public-key distribution system. *Lecture Notes in Computer Science*, 658:458–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580458.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580458.pdf.

Mayers:1998:QCI

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In IEEE [IEE98a], pages 503–509. CODEN ASFPDV. ISBN 0-8186-9172-7 (softbound), 0-7803-5229-7 (casebound), 0-8186-9174-3 (microfiche). ISSN 0272-5428. LCCN QA267 .S95 1998 Sci-Eng. IEEE Catalog Number 98CB36280. IEEE Computer Society Press order number PR9172.

Myers:1994:RIA

[Mye94a] J. Myers. RFC 1731: IMAP4 authentication mechanisms, December 1994. URL ftp://ftp.internic.net/rfc/rfc1731.txt; https://www.math.utah.edu/pub/rfc/rfc1731.txt. Status: PROPOSED STANDARD.

Myers:1994:RPA

[Mye94b] J. Myers. RFC 1734: POP3 AUTHentication command, December 1994. URL ftp://ftp.internic.net/rfc/rfc1734.txt; https://www.math.utah.edu/pub/rfc/rfc1734.txt. Status: PROPOSED STANDARD.

Myers:1996:TAS

[Mye96] Ware Myers. On trial at the Summer Olympic Games: Smart cards. *Computer*, 29 (7):88–91, July 1996. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Myers:1997:RSA

[Mye97] J. Myers. RFC 2222: Simple Authentication and Security Layer (SASL), October 1997. URL ftp://ftp.internic.net/rfc/rfc2222.txt; https://www.math.utah.edu/pub/rfc/rfc2222.txt. Status: PROPOSED STANDARD. Updated by RFC2444 [New98].

Myer:1998:VCS

[Mye98] Charles R. Myer. Viet Cong SIGINT and U.S. Army COMSEC in Vietnam. In Deavours et al. [DKK+98], pages 301–308. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

McCurley:1998:ACE

[MZ98] Kevin S. McCurley and Claus Dieter Ziegler, editors. *Advances in Cryptology, 1981–1997: Electronic Proceedings and Index of the CRYPTO and EUROCRYPT Conferences, 1981–1997*, volume 1440 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. CODEN LNCSD9. ISBN 3-540-65069-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 A373 1998. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1440.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1440`. CD-ROM contains 14692 pages of information from 32 volumes of conference proceedings of CRYPTO and EUROCRYPT.

Mihaljevic:1998:CAB

[MZI98] M. Mihaljevic, Y. Zheng, and H. Imai. A cellular automaton based fast one-way hash function suitable for hardware implementation. *Lecture Notes in Computer Science*, 1431:217–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Merwin:1979:NCC

[MZS79] Richard E. Merwin, Jacqueline T. Zanca, and Merlin. Smith, editors. *1979 National Computer Conference: June 4–7, 1979, New York, New York*, volume 48 of *AFIPS Conference proceedings*. AFIPS Press, Montvale, NJ, USA, 1979.

Nastar:1995:TRD

[NA95] C. Nastar and N. Ayache. Time representation of deformations: Combining vibration modes and Fourier analysis. *Lecture Notes in Computer Science*, 994: 263–276, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nat-Abdesselam:1999:QCA

[NAA99] F. Nat-Abdesselam and N. Agoulmine. QoS control and adaptation in distributed multimedia systems. *Lecture Notes in Computer Science*, 1586: 375–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Naccache:1993:MSF

[Nac93] David Naccache. A Montgomery-suitable Fiat–Shamir-like authentication scheme. *Lecture Notes in Computer Science*, 658: 488–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580488.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580488.pdf.

Nachenberg:1997:CVA

[Nac97] Carey Nachenberg. Computer virus: Antivirus coevolution. *Communications of the Association for Computing Machinery*, 40(1):46–51, January 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/1997-40-1/p46-nachenberg/.

Naik:1989:CDS

[Nai89] Varsha Naik. Cryptology in data security environment: what should be the new trend? Technical report, ????, ????, 1989. 63 pp.

Nalwa:1997:AOS

[Nal97] V. S. Nalwa. Automatic on-line signature verification. *Lecture Notes in Computer Science*, 1351:I–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nanovic:1936:SWI

[Nan36] John Leonard Nanovic. *Secret writing: an introduction to cryptograms, ciphers and codes*. D. Kemp and Co, New York, NY, USA, 1936. x + 117 + 1 pp. LCCN Z104 .N3. See also reprint [Nan74].

Nanovic:1974:SWI

[Nan74] John L. (John Leonard) Nanovic. *Secret writing: an introduction to cryptograms, ciphers, and codes*. Dover Publications, Inc., New York, NY, USA, 1974. ISBN 0-486-23062-7. x + 117 pp. LCCN Z104.N35 1974. Reprint of the 1936 edition [Nan36].

Nastar:1994:VMN

[Nas94] C. Nastar. Vibration modes for nonrigid motion analysis in 3D images. *Lecture Notes in Computer Science*, 800:231–238, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

NBS:1977:DES

[Nat77] National Bureau of Standards. *Data Encryption Standard*. U. S. Department of Commerce, Washington, DC, USA, January 1977. 18 pp.

NBS:1980:MO

[Nat80] National Bureau of Standards. *DES Modes of Operation*. U. S. Department of Commerce, Washington, DC, USA, December 1980. 16 pp.

NCSOTS:1984:ISR

[Nat84] National Communications System (U.S.). Office of Technology and Standards. Interoperability and security requirements for use of the Data Encryption Standard in the physical layer of data communications. Federal standard 1026, General Services Administration, Office of Information Resources Management, Washington, DC, USA, August 3, 1984. various pp.

NIST:1985:FPSa

[Nat85a] National Institute of Standards and Technology. *FIPS PUB 112: Standard for Password Usage*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, May 30, 1985. URL http://www.itl.nist.gov/fipspubs/fip112.htm.

NIST:1985:FPSb

[Nat85b] National Institute of Standards and Technology. *FIPS PUB 113: Standard for Computer Data Authentication*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, May 30, 1985. URL http://www.itl.nist.gov/fipspubs/fip113.htm.

NIST:1991:DSS

[Nat91] National Institute of Standards and Technology. Digital signature standard (DSS). *Federal Register*, 56 (169):??, August 1991. CODEN FEREAC. ISSN 0097-6326.

NIST:1992:DSS

[Nat92a] National Institute of Standards and Technology (NIST). The Digital Signature Standard, proposed by NIST. *Communications of the Association for Computing Machinery*, 35(7):36–40, July 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/129904.html.

NIST:1992:PYA

[Nat92b] National Institute of Standards and Technology (NIST). *Publication YY: Announcement and Specifications for a Secure Hash Standard (SHS)*, January 22 1992. ?? pp.

NIST:1993:FPD

[Nat93a] National Institute of Standards and Technology. *FIPS Publication 46-2: Data Encryption Standard*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, December 1993. ?? pp.

Anonymous:1993:FPD

[Nat93b] National Institute of Standards and Technology (formerly National Bureau of Standards), Gaithersburg, MD, USA. *FIPS Publication 46-2: Data Encryption Standard*, December 30, 1993. ?? pp.

NIST:1993:DES

[Nat93c] National Institute of Standards and Technology (U. S.). *Data encryption standard (DES)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, December 30, 1993. 18 pp. Category: computer security, subcategory: cryptography. Supersedes FIPS PUB 46-1-1988 January 22. Reaffirmed December 30, 1993.

NIST:1994:FPD

[Nat94a] National Institute of Standards and Technology (NIST). *FIPS Publication 186: Digital Signature Standard*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, May 19, 1994. ?? pp.

NIST:1994:DES

[Nat94b] National Institute of Standards and Technology (U. S.). Data Encryption Standard (DES). Federal information processing standards publication 46-2, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 1994. 18 pp. Supersedes FIPS PUB 46-1-1988 January 22. Category: computer security, subcategory: cryptography. Shipping list no.: 94-0171-P. Reaffirmed December 30, 1993.

NIST:1994:DSS

[Nat94c] National Institute of Standards and Technology (U. S.). Digital Signature Standard (DSS). Federal information processing standards publication 186, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, May 19, 1994. 20 pp. Category: computer security, subcategory: cryptography. Shipping list no.: 94-0279-P. Issued May 19, 1994.

NIST:1994:EES

[Nat94d] National Institute of Standards and Technology (U.

S.). Escrowed Encryption Standard (EES). Federal information processing standards publication 185, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 1994. 7 pp. Category: computer security, subcategory: cryptography. Shipping list no.: 94-0159. Issued February 9, 1994.

NIST:1995:FPSb

[Nat95] National Institute of Standards and Technology. *FIPS PUB 180-1: Secure Hash Standard*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, April 17, 1995. URL `http://www.itl.nist.gov/fipspubs/fip180-1.htm`. Supersedes FIPS PUB 180 1993 May 11.

Natarajan:1997:RPK

[Nat97a] Balas Natarajan. Robust public key watermarking of digital images. Technical Report 97-118, HP Laboratories, October 1997. 10 pp.

NIST:1997:ARC

[Nat97b] National Institute of Standards and Technology. Announcing request for candidate algorithm nominations for the Advanced Encryption Standard (AES). *Federal Register*, 62(177): 48051–48058, September 12, 1997. CODEN FEREAC. ISSN 0097-6326.

NIST:1998:FAE

[Nat98] National Institute of Standards and Technology, editor. *The First Advanced Encryption Standard Candidate Conference, August 20–22, 1998, DoubleTree Hotel, Ventura, California*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 1998. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf1/aes1conf.htm; http://www.nist.gov/aes`. See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

NIST:1999:FPD

[Nat99a] National Institute of Standards and Technology. *FIPS PUB 46-3: Data Encryption Standard (DES)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, October 25, 1999. URL `http://www.itl.nist.gov/fipspubs/fip186-2.pdf`. supersedes FIPS 46-2.

NIST:1999:SAC

[Nat99b] National Institute of Standards and Technology, editor. *Second AES Candidate Conference Proceedings, March 22–23, 1999, Rome, Italy*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, March 1999. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen "complete and proper" candidates.

NIST:1999:SRF

[Nat99c] National Institute of Standards and Technology. Status report on the first round of the development of the Advanced Encryption Standard. Technical report, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, August 1999. ???? pp.

NIST:19xx:AES

[Natxx] National Institute of Standards and Technology. *Advanced Encryption Standard (AES) Development Effort*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 19xx. ?? pp. URL http://csrc.nist.gov/encryption/aes/aes_home.htm.

Nechvatal:1999:SRF

[NBD+99] James Nechvatal, Elaine Barker, Donna Dodson, Morris Dworkin, James Foti, and Edward Roback. Status report on the first round of the development of the Advanced Encryption Standard. *Journal of research of the National Institute of Standards and Technology*, 104 (5):435–460, 1999. CODEN JRITEF. ISSN 1044-677X (print), 2165-7254 (electronic). URL http://citeseer.nj.nec.com/nechvatal99status.html; http://csrc.nist.gov/encryption/aes/round1/r1report.htm.

NBS:1975:EAC

[NBS75a] NBS. Encryption algorithm for computer data protection: requests for comments. *Federal Register*, 40(??):12134–??, March 17, 1975. CODEN FEREAC. ISSN 0097-6326.

NBS:1975:NPF

[NBS75b] NBS. Notice of a proposed federal information processing Data Encryption Standard. *Federal Register*, 40 (??):12607–??, August 12, 1975. CODEN FEREAC. ISSN 0097-6326.

NBS:1976:NWC

[NBS76] NBS. The NBS workshop on cryptography in support of computer security. Unpublished memorandum, U.S. National Bureau of Standards, Gaithersburg, MD, USA, September 1976.

Nilsson:1978:OST

[NBWH78] Arne Nilsson, Rolf Blom, Harald Wesemeyer, and S. Hellstrom. On overflow systems in telephone networks: general service times in the secondary group. *Ericsson technics*, 34(2):48–128, 1978.

Nandi:1997:RCT

[NC97] S. Nandi and P. P. Chaudhuri. Reply to comments on "Theory And Application Of Cellular Automata In Cryptography". *IEEE Transactions on Computers*, 46(5):639, May 1997. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=589246. See [NKC94, BMP+97b].

Neat:1975:NCC

[Nea75] Charlie Edmund Neat. *A new computer cryptography: the Expanded Character Set (ECS) cipher*. PhD thesis, Engineering, University of California, Los Angeles, Los Angeles, CA, USA, 1975. xxi + 203 pp.

Nechvatal:1991:PC

[Nec91] James Nechvatal. *Public-key cryptography*. NIST special publication: Computer security 800-2. U.S. Dept. of Commerce, National Institute of Standards and Technology, Washington, DC, USA, April 1991. ix + 162 pp. LCCN QC 100 U57 no.800-2 1991 Microfiche. Microfiche.

Nechvatal:1996:PKB

[Nec96] James Nechvatal. A public-key-based key escrow system. *The Journal of Systems and Software*, 35(1): 73–83, October 1996. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Needham:1994:DSE

[Nee94] Roger M. Needham. Denial of service: an example. *Communications of the Association for Computing Machinery*, 37(11): 42–46, November 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/188294.html.

NetworkAssociates:1998:NB

[Net98] Network Associates, Inc. Nuts and bolts, 1998. Includes CD-ROM and book.

Neumann:1991:IRCd

[Neu91] Peter G. Neumann. Inside RISKS: Collaborative efforts. *Communications of the Association for Computing Machinery*, 34(12): 162, December 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/125411.html.

Neumann:1992:IRF

[Neu92] Peter G. Neumann. Inside RISKS: Fraud by computer. *Communications of the Association for Computing Machinery*, 35(8): 154, August 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/135238.html.

Neumann:1994:IRA

[Neu94] Peter G. Neumann. Inside RISKS: Alternative passwords. *Communications of the Association for Computing Machinery*, 37(5): 146, May 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/175311.html.

Neumann:1995:RCD

[Neu95] Peter G. Neumann. Reassessing the crypto debate. *Communications of the Association for Computing Machinery*, 38(3): 138, March 1995. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/203352.html.

Neumann:1997:IRC

[Neu97] Peter G. Neumann. Inside risks: Crypto key management. *Communications of the Association for Computing Machinery*, 40(8): 136, August 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/1997-40-8/p136-neumann/.

Newton:1997:EC

[New97] David E. Newton. *Encyclopedia of cryptology*. ABC-CLIO, Santa Barbara, CA, USA, 1997. ISBN 0-87436-772-7. xi + 330 pp. LCCN Z 103 N344 1997.

Newman:1998:ROT

[New98] C. Newman. RFC 2444: The one-time-password SASL mechanism, October 1998.

URL ftp://ftp.internic.net/rfc/rfc2222.txt; ftp://ftp.internic.net/rfc/rfc2444.txt; https://www.math.utah.edu/pub/rfc/rfc2222.txt; https://www.math.utah.edu/pub/rfc/rfc2444.txt. Updates RFC2222 [MR95b]. Status: PROPOSED STANDARD.

Neve:1999:FSC

[NFQ99] Amaury Nève, Denis Flandre, and Jean-Jacques Quisquater. Feasibility of Smart Cards in silicon-on-insulator (SOI) technology. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL http://www.usenix.org/publications/library/proceedings/smartcard99/neve.html.

Ng:1999:CST

[Ng99] Siaw-Lynn Ng. Comments on "On the Security of Three-Party Cryptographic Protocols" by Xu, Zhang, Zhu. *Operating Systems Review*, 33(3):5–6, July 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic). See [XZZ98].

Nguyen:1999:CGC

[Ngu99a] P. Nguyen. Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto '97. In Wiener [Wie99], pages 288–304. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Nguyen:1999:CGG

[Ngu99b] P. Nguyen. Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto '97. *Lecture Notes in Computer Science*, 1666: 288–304, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nelson:1990:SAE

[NH90] Ruth Nelson and John Heimann. SDNS architecture and end-to-end encryption. *Lecture Notes in Computer Science*, 435: 356–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350356.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350356.pdf.

Neubauer:1998:DWI

[NH98] C. Neubauer and J. Herre. Digital watermarking and its influence on audio quality. In Anonymous [Ano98n], page ?? LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1053.html.

Neubauer:1998:CSD

[NHB98] Chr. Neubauer, J. Herre, and K. Brandenburg. Continuous steganographic data transmission using uncompressed audio. *Lecture Notes in Computer Science*, 1525:208–217, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250208.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250208.pdf`.

Nichols:1998:CCCa

[Nic98a] Randall K. Nichols. *Classical Cryptography Course*, volume 1. Aegean Park Press, Laguna Hills, CA, USA, November 1998. ISBN 0-89412-263-0. 301 (est.) pp. US$36.80.

Nichols:1998:CCCb

[Nic98b] Randall K. Nichols. *Classical Cryptography Course*, volume 2. Aegean Park Press, Laguna Hills, CA, USA, November 1998. ISBN 0-89412-264-9. 452 pp. US$42.80.

Nichols:1999:IGC

[Nic99] Randall K. Nichols. *ICSA guide to cryptography*. McGraw-Hill, New York, NY, USA, 1999. ISBN 0-07-913759-8 (paperback). xxxix + 837 pp. LCCN QA76.9.A25 N53 1999 Accompanying CD-Rom is shelved in Reserves.

Niederreiter:1986:KTC

[Nie86] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 15(2):159–166, 1986. CODEN PUTIAI. ISSN 0370-2529.

Niederreiter:1988:SNC

[Nie88] Harald Niederreiter. Some new cryptosystems based on feedback shift register sequences. *Math. J. Okayama Univ.*, 30:121–149, 1988. CODEN MJOKAP. ISSN 0030-1566.

NIST:1985:FPC

[NIS85] NIST. *FIPS PUB 113: Computer Data Authentication*. National Institute of Standards and Technology (formerly National Bureau of Standards), Gaithersburg, MD, USA, May 30, 1985. ?? pp.

Nissan:1989:AIM

[Nis89] Ephraim Nissan. Artificial intelligence for a metatheory of interpretation. (A knowledge-analysis of Bernardini Marzolla's Indoglottal interpretation of Etruscan: For a metamodel of interpretation). Technical Report Report, 133

p. (available from the author), CMS, Univ. of Greenwich, Woolwich, London, UK, 1989.

Nissan:1991:EMF

[Nis91] Ephraim Nissan. Etruscan [computer models for]. In Ian Lancashire, editor, *The Humanities Computing Yearbook, 1989–90*, page 246. Clarendon Press, Oxford, UK, 1991.

NIST:1992:NCS

[NIS92] NIST, editor. *15th National Computer Security Conference: October 13–16, 1992, Baltimore Convention Center, Baltimore, MD: information systems security, building blocks to the future*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 1992. LCCN QA76.9.A25 N38 1992. Two volumes.

Nist:1993:DSS

[NIS93a] NIST. *Digital Signature Standard*. Gaithersburg, MD 20899-8900, USA, February 1, 1993. ?? pp. FIPS PUB 186.

NIST:1993:FPS

[NIS93b] NIST. *FIPS PUB 180: Secure Hash Standard (SHS)*. National Institute of Standards and Technology, Gaithersburg, MD, USA, May 11, 1993. ?? pp.

Anonymous:1994:DSS

[NIS94] NIST, U. S. Department of Commerce, Washington, DC, USA. *Digital Signature Standard*, May 1994. ?? pp. FIPS PUB 186.

Nisan:1996:ERH

[Nis96] N. Nisan. Extracting randomness: How and why, a survey. In Cai and Homer [CH96], pages 44–58. ISBN 0-8186-7386-9, 0-8186-7387-7. LCCN QA267 .S765 1996; QA267.7 .I34 1996. IEEE catalog number 96CB3591.

Nyberg:1993:PSA

[NK93] K. Nyberg and L. R. Knudsen. Probable security against differential cryptanalysis. *Lecture Notes in Computer Science*, 740: 566–574, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nakamura:1998:MEC

[NK98a] D. Nakamura and K. Kobayashi. Modified ElGamal cryptosystem. *Lecture Notes in Computer Science*, 1396: 96–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nikander:1998:JBC

[NK98b] Pekka Nikander and Arto Karila. A Java beans component architecture for cryptographic protocols. In USENIX [USE98d], page ?? ISBN 1-880446-92-8. LCCN QA76.9.A25 U83 1998. URL http://www.usenix.org/publications/library/proceedings/sec98/nikander.html.

Nandi:1994:TAC

[NKC94] S. Nandi, B. K. Kar, and P. Pal Chaudhuri. Theory and applications of cellular automata in cryptography. *IEEE Transactions on Computers*, 43(12): 1346–1357, December 1994. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=338094.

Nikander:1999:PPD

[NKP99] P. Nikander, Y. Kortesniemi, and J. Partanen. Preserving privacy in distributed delegation with fast certificates. *Lecture Notes in Computer Science*, 1560:136–153, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nakamura:1988:DRM

[NM88] Yasuhiro Nakamura and Kineo Matsui. Dual reduction method of random keys for encryption by graph transformation. *Mem. Nat. Defense Acad.*, 28(1):39–51, 1988. CODEN MDPCAW. ISSN 0388-4112.

Naccache:1994:MSC

[NM94] David Naccache and David M'Raïhi. Montgomery-suitable cryptosystems. *Lecture Notes in Computer Science*, 781:75–81, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Naccache:1996:ACP

[NM96a] David Naccache and David M'Raïhi. Arithmetic coprocessors for public-key cryptography: The state of the art. In P. H. Hartel, P. Paradinas, and J.-J. Quisquater, editors, *Proceedings of CARDIS 96, Amsterdam, The Netherlands, September 16–18, 1996*, pages 14–24. ????, ????, 1996. URL https://pdfs.semanticscholar.org/92c2/0b1417b1a51c71189fb8ac8fcd7fba1faee9.pdf.

Naccache:1996:CSC

[NM96b] David Naccache and David M'Raïhi. Cryptographic smart cards — comparing the existing cryptography-dedicated microprocessors and describing possible directions for their evolution. *IEEE Micro*, 16(3): 14, 16–24, May/June 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Nadathur:1999:SDT

[NM99] G. Nadathur and D. J. Mitchell. System description: Teyjus — a compiler and abstract machine based implementation of lambdaProlog. *Lecture Notes in Computer Science*, 1632: 287–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Naccache:1995:CMP

[NMR95] David Naccache, David M'Raïhi, and Dan Raphaeli. Can Montgomery parasites be avoided? A design methodology based on key and cryptosystem modifications. *Designs, Codes, and Cryptography*, 5(1):73–80, January 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/BF01388505; http://www.wkap.nl/oasis.htm/77820.

Nguyen:1998:NDC

[NMV98] Khanh Quoc Nguyen, Y. Mu, and V. Varadharajan. A new digital cash scheme based on blind Nyberg-Rueppel digital signature. *Lecture Notes in Computer Science*, 1396:313–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1999:DZK

[NMV99] Khanh Quoc Nguyen, Y. Mu, and V. Varadharajan. Divertible zero-knowledge proof of polynomial relations and blind group signature. *Lecture Notes in Computer Science*, 1587:117–128, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Naccache:1995:CDB

[NMVR95a] D. Naccache, D. M'Raihi, S. Vaudenay, and D. Raphaeli. Can D.S.A. be improved? complexity trade-offs with the digital signature standard. *Lecture Notes in Computer Science*, 950: 77–85, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Naccache:1995:CDI

[NMVR95b] David Naccache, David M'Raïhi, Serge Vaudenay, and Dan Raphaeli. Can D.S.A. be improved? complexity trade-offs with the Digital Signature Standard. *Lecture Notes in Computer Science*, 950: 77–85, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500077.htm; http://link.springer-ny.com/link/service/series/

0558/papers/0950/09500077.pdf.

Nozaki:1997:LCS

[NNEK97] K. Nozaki, M. Niimi, R. O. Eason, and E. Kawaguchi. A large capacity steganography using color BMP images. *Lecture Notes in Computer Science*, 1351:I–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Noras:1996:CHH

[NO96] J. M. Noras and J. Omar. Customising hardware for high-performance block ciphering. In ????, editor, *REDECS '96, National Conference on Research and Development in Computer Science and its Applications, June 26-27, Universiti Pertanian Malaysia, Selangor.*, page ?? ????, ????, 1996. ISBN ???? LCCN ????

Nicchiotti:1998:NIS

[NO98] G. Nicchiotti and E. Ottaviano. Non-invertible statistical wavelet watermarking. In Theodoridis et al. [T+98], pages 2289–2292. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073157.html. Four volumes.

Nobauer:1984:CRS

[Nöb84] Rupert Nöbauer. Cryptanalysis of the Rédei-scheme. In Eigenthaler et al. [EKMN84], pages 255–264. ISBN 3-209-00591-5, 3-519-02762-3. LCCN ????

Nobauer:1985:CRS

[Nöb85] Rupert Nöbauer. Cryptanalysis of the Rédei-scheme. In *Contributions to general algebra, 3 (Vienna, 1984)*, pages 255–264. Hölder-Pichler-Tempsky, Vienna, Austria, 1985.

Nobauer:1988:CPK

[Nöb88] Rupert Nöbauer. Cryptanalysis of a public-key cryptosystem based on Dickson-polynomials. *Mathematica Slovaca*, 38(4): 309–323, 1988. CODEN MASLDM. ISSN 0139-9918.

Norman:1973:SWB

[Nor73] Bruce Norman. *Secret warfare: the battle of codes and ciphers.* David and Charles, Newton Abbot, UK, 1973. ISBN 0-7153-6223-2. 187 pp. LCCN Z103 .N67.

Noras:1995:CHHa

[Nor95a] J. M. Noras. Ciphering hardware for high-speed digital networks: A REDOC III implementation. *IEE Electronics Letters*, 31 (11):851–852, June 1995.

Noras:1995:CHHb

[Nor95b] J. M. Noras. Custom hardware for high performance and high security digital data ciphering. In ????, editor, *European Convention on Security and Detection (ECOS '95), Brighton, 16–18 May 1995*, pages 128–132. ????, ????, 1995. ISBN ???? LCCN ????

Noras:1995:PCE

[Nor95c] J. M. Noras. Potential of customer encryption hardware with FGPAs. In ????, editor, *Educational ECAS User Group Workshop, Napier University, 12th September 1995*, page ???? ????, ????, 1995. ISBN ???? LCCN ????

Naor:1993:PZK

[NOVY93] M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung. Perfect zero-knowledge arguments for NP can be based on general complexity assumptions. *Lecture Notes in Computer Science*, 740:196–214, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Naor:1997:VAI

[NP97] Moni Naor and Benny Pinkas. Visual authentication and identification. *Lecture Notes in Computer Science*, 1294: 322–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940322.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940322.pdf.

Naor:1998:TTT

[NP98a] M. Naor and B. Pinkas. Threshold traitor tracing. *Lecture Notes in Computer Science*, 1462: 502–517, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073609.html.

Nikolaidis:1998:RIW

[NP98b] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. *Signal Processing*, 66(3):385–403, May 1998. CODEN SPRODR. ISSN 0165-1684. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073158.html.

Naor:1999:OTA

[NP99] M. Naor and B. Pinkas. Oblivious transfer with adaptive queries. In Wiener [Wie99], pages 573–590. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Niemi:1994:CPV

[NR94] V. Niemi and A. Renvall. Cryptographic protocols and voting. *Lecture Notes in Computer Science*, 812:307–316, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nyberg:1995:MRS

[NR95] K. Nyberg and R. A. Rueppel. Message recovery for signature schemes based on the discrete logarithm problem. *Lecture Notes in Computer Science*, 950:182–193, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Naor:1998:UIS

[NR98] M. Naor and O. Reingold. From unpredictability to indistinguishability: a simple construction of pseudo-random functions from MACs. *Lecture Notes in Computer Science*, 1462: 267–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Needham:1978:UEAa

[NS78a] R. M. (Roger Michael) Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. Technical Report CSL-78-4, Xerox Palo Alto Research Center, Palo Alto, CA, USA, 1978. ?? pp. Reprinted June 1982.

Needham:1978:UEAb

[NS78b] Roger M. Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the Association for Computing Machinery*, 21(12):993–999, December 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Needham:1987:AR

[NS87] R. M. Needham and M. D. Schroeder. Authentication revisited. *Operating Systems Review*, 21(1):7, January 1987. CODEN OSRED8. ISSN 0163-5980.

Neuman:1988:AUE

[NS88] B. Clifford Neuman and Jennifer G. Steiner. Authentication of unknown entities on an insecure network of untrusted workstations. In USENIX Association [USE88b], pages 10–11. LCCN QA76.8.U65 U55 1988(1)-1990(2)//. Abstract only.

Norris-Saucedo:1989:DAD

[NS89] Steven Joseph Norris-Saucedo. Development and application of data encryption using a data shuffling technique. Thesis (M.S.), Department of Electrical Engineering, University of Colorado at Denver, Denver, CO, USA, 1989. vii + 94 pp.

Naor:1995:VC

[NS95] M. Naor and A. Shamir. Visual cryptography. *Lecture Notes in Computer Science*, 950:1–12, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/032134.html.

Naccache:1997:NPK

[NS97a] David Naccache and Jacques Stern. A new public-key cryptosystem. *Lecture Notes in Computer Science*, 1233:27–36, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330027.htm; http://link.springer-ny.com/link/service/series/0558/papers/1233/12330027.pdf.

Nguyen:1997:MRC

[NS97b] P. Nguyen and J. Stern. Merkle–Hellman revisited: a cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations. *Lecture Notes in Computer Science*, 1294: 198–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1997:MHR

[NS97c] Phong Nguyen and Jacques Stern. Merkle–Hellman revisited: a cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations. *Lecture Notes in Computer Science*, 1294: 198–212, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nechaev:1998:DSB

[NS98a] Y. I. Nechaev and Y. L. Siek. Design of ship-board control system based on the soft computing conception. *Lecture Notes in Computer Science*, 1416: 192–199, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1998:BQS

[NS98b] P. Nguyen and J. Stern. The Beguin–Quisquater server-aided RSA protocol from Crypto'95 is not secure. *Lecture Notes in Computer Science*, 1514:372–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1998:BSR

[NS98c] P. Nguyen and J. Stern. The Beguin-Quisquater server-aided RSA protocol from Crypto'95 is not secure. *Lecture Notes in Computer Science*, 1514:372–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1998:CAC

[NS98d] P. Nguyen and J. Stern. Cryptanalysis of the Ajtai–Dwork cryptosystem. *Lecture Notes in Computer Science*, 1462:223–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1998:CAD

[NS98e] Phong Nguyen and Jacques Stern. Cryptanalysis of the Ajtai–Dwork cryptosystem. *Lecture Notes in Computer Science*, 1462: 223–242, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1999:CFP

[NS99a] P. Nguyen and J. Stern. Cryptanalysis of a fast public key cryptosystem presented at SAC '97. *Lecture Notes in Computer Science*, 1556:213–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1999:HHS

[NS99b] P. Nguyen and J. Stern. The hardness of the hidden subset sum problem and its cryptographic implications. In Wiener [Wie99], pages 31–46. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Naccache:1999:HCF

[NSS99] D. Naccache, A. Shamir, and J. P. Stern. How to copyright a function ? *Lecture Notes in Computer Science*, 1560:188–196, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nieh:1993:MAC

[NT93] B. B. Nieh and S. E. Tavares. Modelling and analyzing cryptographic protocols using Petri nets. *Lecture Notes in Computer Science*, 718:275–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Neuman:1994:KAS

[NT94] B. Clifford Neuman and Theodore Y. Ts'o. Kerberos: an authentication service for computer networks. ISI reprint series ISI/RS-94-399, University of Southern California, Information Sciences Institute, Marina del Rey, CA, USA, 1994. 6 pp. Reprinted, with permission, from IEEE Communications Magazine, Volume 32, Number 9, pages 33–38, September 1994.

Nadjm-Tehrani:1999:BHO

[NT99] S. Nadjm-Tehrani. Building hybrid observers for complex dynamic systems using model abstractions integration of analog and discrete synchronous design. *Lecture Notes in Computer Science*, 1569:193–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nemetz:1988:RLS

[NU88] T. Nemetz and J. Ureczky. A random linear secret-key encryption. In *Probability theory and mathematical statistics with applications (Visegrád, 1985)*, pages 171–180. D. Reidel, Dordrecht, Boston, Lancaster, Tokyo, 1988.

Nurmi:1994:CPA

[Nur94] H. Nurmi. Cryptographic protocols for auctions and bargaining. *Lecture Notes in Computer Science*, 812: 317–324, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Needham:1997:TE

[NW97] Roger M. Needham and David J. Wheeler. TEA extensions. Report, Cambridge University, Cambridge, UK, October 1997. URL `http://www.movable-type.co.uk/scripts/xtea.pdf`. See also original TEA [WN95] and extension XXTEA [WN98a].

Naor:1998:ACS

[NW98] M. Naor and A. Wool. Access control and signatures via quorum secret sharing. *IEEE Transactions on Parallel and Distributed Systems*, 9(9):909–??, September 1998. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://dlib.computer.org/td/books/td1998/pdf/l0909.pdf`; `http://www.computer.org/tpds/td1998/l0909abs.htm`.

Naor:1989:UOW

[NY89a] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In ACM-TOC'89 [ACM89c], pages 33–43. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. URL `http://www.acm.org/pubs/articles/proceedings/stoc/73007/p33-naor/p33-naor.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/73007/p33-naor/`.

Naor:1989:UOH

[NY89b] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In ACM-TOC'89 [ACM89c], pages 33–43. ISBN 0-89791-

307-8. LCCN QA 76.6 A13 1989.

Naor:1990:PKC

[NY90] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In ACM [ACM90], pages 427–437. ISBN 0-89791-361-2. LCCN QA76.A15 1990. URL `http://www.acm.org/pubs/citations/proceedings/stoc/100216/p427-naor/`. ACM order no. 508900.

Nyberg:1994:DUM

[Nyb94] K. Nyberg. Differentially uniform mappings for cryptography. *Lecture Notes in Computer Science*, 765: 55–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nyberg:1995:LAB

[Nyb95] K. Nyberg. Linear approximation of block ciphers. *Lecture Notes in Computer Science*, 950:439–444, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nyberg:1998:ACE

[Nyb98] Kaisa Nyberg, editor. *Advances in cryptology: EUROCRYPT '98: International Conference on the theory and application of cryptographic techniques, Espoo, Finland, May 31 — June 4, 1998: proceedings*, volume 1403 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-64518-7 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1403.

Nystrom:1999:PCT

[Nys99] Magnus Nyström. PKCS #15 — a cryptographic-token information format standard. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL `http://www.usenix.org/publications/library/proceedings/smartcard99/nystrom.html`.

Ohta:1994:LCF

[OA94] Kazuo Ohta and Kazumaro Aoki. Linear cryptanalysis of the Fast Data Encipherment Algorithm. In Desmedt [Des94b], pages 12–16. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390012.htm`; `http://link.springer-ny.com/link/service/series/`

0558/papers/0839/08390012.pdf.

Ohsuga:1999:EHI

[OA99] S. Ohsuga and T. Aida. Externalization of human idea and problem description for automatic programming. *Lecture Notes in Computer Science*, 1609: 163–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Oakley:1978:RPC

[Oak78] Howard T. Oakley. *The Riverbank publications on cryptology*. ????, Washington, DC, USA, 1978. 324–330 pp.

Oberzalek:1999:GEE

[Obe99] Martin Oberzalek. genigma: Enigma emulator. GPL-licensed software., 1999. URL http://home.pages.at/kingleo/genigma-1.2.tar.gz; http://home.pages.at/kingleo/programme_gnome_en.html.

OConnell:1981:CDE

[O'C81] Richard O'Connell. *Cryptoease: a data encryption dictionary*. Atlantis Editions, Philadelphia, PA, USA, 1981. 33 pp.

OConnor:1994:UBN

[O'C94] Luke O'Connor. An upper bound on the number of functions satisfying the Strict Avalanche Criterion. *Information Processing Letters*, 52(6):325–327, December 23, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

OConnor:1995:DCT

[O'C95] L. O'Connor. A differential cryptanalysis of tree-structured substitution-permutation networks. *IEEE Transactions on Computers*, 44(9):1150–1152, September 1995. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=464394.

Obenland:1999:SED

[OD99] K. M. Obenland and A. M. Despain. Simulating the effect of decoherence and inaccuracies on a quantum computer. *Lecture Notes in Computer Science*, 1509: 447–459, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

ORuanaidh:1996:PWD

[ODB96] J. J. K. O'Ruanaidh, W. J. Dowling, and F. M. Boland. Phase watermarking of digital images. In IEEE [IEE96e], pages 239–242. ISBN 0-7803-3258-X (softbound), 0-7803-3259-8 (casebound), 0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM). LCCN TK8315.I222 1996. Three volumes. IEEE catalog number 96CH35919.

Odlyzko:1984:CAM

[Odl84] Andrew M. Odlyzko. Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme. *IEEE Transactions on Information Theory*, IT-30(4):594–601, 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL `http://www.research.att.com/~amo/doc/arch/knapsack.attacks.pdf`; `http://www.research.att.com/~amo/doc/arch/knapsack.attacks.ps`; `http://www.research.att.com/~amo/doc/arch/knapsack.attacks.troff`.

Odlyzko:1985:DLF

[Odl85] A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In Beth et al. [BCI85], pages 224–314. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL `http://www.research.att.com/~amo/doc/arch/discrete.logs.pdf`; `http://www.research.att.com/~amo/doc/arch/discrete.logs.ps`; `http://www.research.att.com/~amo/doc/arch/discrete.logs.troff`. Held at the University of Paris, Sorbonne.

Odlyzko:1987:CCD

[Odl87a] A. M. Odlyzko. On the complexity of computing discrete logarithms and factoring integers. In Cover and Gopinath [CG87], pages 113–116. ISBN 0-387-96621-8. LCCN TK5102.5 .O243 1987. US$25.00. URL `http://www.research.att.com/~amo/doc/arch/factoring.logs.pdf`; `http://www.research.att.com/~amo/doc/arch/factoring.logs.ps`; `http://www.research.att.com/~amo/doc/arch/factoring.logs.troff`.

Odlyzko:1987:ACC

[Odl87b] Andrew Michael Odlyzko, editor. *Advances in cryptology: CRYPTO '86: proceedings*, volume 263 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL `http://link.springer-ny.com/link/service/series/`

0558/tocs/t0263.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Odlyzko:1990:RFK

[Odl90] A. M. Odlyzko. The rise and fall of knapsack cryptosystems. In Pomerance and Goldwasser [PG90], pages 75–88. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. URL http://www.research.att.com/~amo/doc/arch/knapsack.survey.pdf; http://www.research.att.com/~amo/doc/arch/knapsack.survey.ps; http://www.research.att.com/~amo/doc/arch/knapsack.survey.troff. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

Odlyzko:1994:DLS

[Odl94a] A. M. Odlyzko. Discrete logarithms and smooth polynomials. In Gary L. Mullen, P. Shiue, et al., editors, *Finite Fields: Theory, Applications and Algorithms*, volume 168 of *Contemporary mathematics (American Mathematical Society)*, pages 269–278. American Mathematical Society, Providence, RI, USA, 1994. ISBN 0-8218-5183-7. LCCN QA247.3 .I58 1993.

Odlyzko:1994:PKC

[Odl94b] Andrew M. Odlyzko. Public key cryptography. *AT&T Technical Journal*, 73(5): 17–23, September/October 1994. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic). URL http://www.research.att.com/~amo/doc/arch/public.key.crypto.pdf; http://www.research.att.com/~amo/doc/arch/public.key.crypto.ps; http://www.research.att.com/~amo/doc/arch/public.key.crypto.tex.

Odlyzko:1995:FIF

[Odl95] Andrew M. Odlyzko. The future of integer factorization. *CryptoBytes*, 1(2):5–12, Summer 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf; http://www.research.att.com/~amo/doc/future.of.factoring.pdf; http://www.research.att.com/~amo/doc/future.of.factoring.ps; http://www.research.att.com/~amo/doc/future.of.factoring.tex.

Odlyzko:1998:C

[Odl98] A. M. Odlyzko. Crypto '86.

Lecture Notes in Computer Science, 1440:61–68, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Oelke:1997:VDE

[Oel97] Thomas Oelke. VHDL design of a DES encryption cracking system. Thesis (M.S.), Rochester Institute of Technology, Rochester, NY, USA, 1997. ix + 114 pp.

Okamoto:1993:EDS

[OFF93] Tatsuaki Okamoto, Atsushi Fujioka, and Eiichiro Fujisaki. An efficient digital signature scheme based on an elliptic curve over the ring Z_n. *Lecture Notes in Computer Science*, 740: 54–65, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0740/07400054.htm; http://link.springer-ny.com/link/service/series/0558/papers/0740/07400054.pdf`.

OConnor:1995:UMA

[OG95] Luke O'Connor and Jovan Dj. Golić. A unified Markov approach to differential and linear cryptanalysis. *Lecture Notes in Computer Science*, 917: 387–397, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Oehler:1997:RHM

[OG97] M. Oehler and R. Glenn. RFC 2085: HMAC-MD5 IP authentication with replay prevention, February 1997. URL `ftp://ftp.internic.net/rfc/rfc2085.txt; https://www.math.utah.edu/pub/rfc/rfc2085.txt`. Status: PROPOSED STANDARD.

Oh:1999:DCT

[Oh99] A. Oh. The design of cooperative transaction model by using client-server architecture. *Lecture Notes in Computer Science*, 1626: 269–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ohira:1999:EDD

[Ohi99] Toru Ohira. Encryption with delayed dynamics. *Computer Physics Communications*, 121–122:54–56, September/October 1999. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465599002799`.

Ohta:1996:DCT

[Oht96] Naohisa Ohta, editor. *Digital compression technologies and systems for video* *communications: 7–9 October 1996, Berlin, FRG*, volume 2952 of *Proceedings of SPIE—the International Society for Optical Engineering*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 1996. CODEN PSISDG. ISBN 0-8194-2356-4. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TA1637 .D53 1996.

Ohta:1998:RBD

[Oht98] K. Ohta. Remarks on blind decryption. *Lecture Notes in Computer Science*, 1396: 109–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ohta:1998:ACA

[OiDP98] Kazuo Ohta and Ting i (Dingyi) Pei, editors. *Advances in cryptology — Asiacrypt'98: International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China, October 18–22, 1998: proceedings*, volume 1514 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-65109-8 (softcover). LCCN QA76.9.A25I5553 1998.

Okada:1995:LBS

[OK95] K. Okada and K. Kurosawa. Lower bound on the size of shares of nonperfect secret sharing schemes. *Lecture Notes in Computer Science*, 917:33–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Obana:1996:VIS

[OK96a] Satoshi Obana and Kaoru Kurosawa. Veto is impossible in secret sharing schemes. *Information Processing Letters*, 58(6):293–295, June 24, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ogata:1996:OSS

[OK96b] W. Ogata and K. Kurosawa. Optimum secret sharing scheme secure against cheating. *Lecture Notes in Computer Science*, 1070: 200–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ogata:1998:SBP

[OK98] W. Ogata and K. Kurosawa. Some basic properties of general nonperfect secret sharing schemes. *J.UCS: Journal of Universal Computer Science*, 4(8): 690–??, August 28, 1998. ISSN 0948-6968. URL http://medoc.springer.de:8000/jucs/jucs_4_8/some_basic_properties_of.

Okamoto:1988:DMS

[Oka88] Tatsuaki Okamoto. A digital multisignature scheme using bijective public-key cryptosystems. *ACM Transactions on Computer Systems*, 6(4):432–441, November 1988. CODEN ACSYEC. ISSN 0734-2071. URL http://www.acm.org:80/pubs/citations/journals/tocs/1988-6-4/p432-okamoto/.

Okamoto:1993:RAC

[Oka93a] T. Okamoto. On the relationship among cryptographic physical assumptions. *Lecture Notes in Computer Science*, 762: 369–378, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Okamoto:1993:PSP

[Oka93b] T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. *Lecture Notes in Computer Science*, 740: 31–53, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Okamoto:1994:DCS

[Oka94] Tatsuaki Okamoto. Designated confirmer signatures and public-key encryption are equivalent. In Desmedt [Des94b], pages 61–74. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390061.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390061.pdf.

Okamoto:1998:TKR

[Oka98a] T. Okamoto. Threshold key-recovery systems for RSA. *Lecture Notes in Computer Science*, 1361: 191–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Okamoto:1998:TKS

[Oka98b] T. Okamoto. Threshold key-recovery systems for RSA. *Lecture Notes in Computer Science*, 1361: 191–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Okon:1996:DWN

[Oko96] Chris Okon. Digital watermarking: New techniques for image ownership branding. *Advanced Imaging*, 11 (10), October 1996. CODEN ADIMEZ. ISSN 1042-0711.

Okon:1997:KMA

[Oko97] Chris Okon. Keeping up multimedia asset value. *Advanced Imaging*, 12(7):42–43, July 1997. CODEN ADIMEZ. ISSN 1042-0711.

Ogata:1997:FTA

[OKST97] W. Ogata, K. Kurosawa, K. Sako, and K. Takatani. Fault tolerant anonymous channel. In Han et al. [HOQ97], pages 440–444. CODEN LNCSD9. ISBN 3-540-63696-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I554 1997. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064437.html`.

Ogata:1993:NSS

[OKT93] W. Ogata, K. Kurosawa, and S. Tsujii. Nonperfect secret sharing schemes. *Lecture Notes in Computer Science*, 718:56–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Oleshchuk:1995:PKC

[Ole95] Vladimir A. Oleshchuk. On public-key cryptosystem based on Church–Rosser string-rewriting systems (extended abstract). *Lecture Notes in Computer Science*, 959:264–269, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Oldehoeft:1984:SSU

[OM84] Arthur E. Oldehoeft and Robert McDonald. A software scheme for user-controlled file encryption. *Computers and Security*, 3 (1):35–41, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900245`.

Ohta:1994:DAM

[OM94] Kazuo Ohta and Mitsuru Matsui. Differential attack on message authentication codes. *Lecture Notes in Computer Science*, 773:200–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730200.htm; http://link.springer-ny.com/link/service/series/0558/papers/0773/07730200.pdf`.

Ohbuchi:1997:WTP

[OMA97] Ryutarou Ohbuchi, Hiroshi Masuda, and Masaki Aono. Watermarking three-dimensional polygonal models. In Hollan and Foley [HF97], pages 261–272. ISBN 0-201-32232-3, 0-89791-991-2 (ACM). LCCN QA76.575.A36 1997. ACM order number 433971.

Ohbuchi:1998:WTD

[OMA98] Ryutarou Ohbuchi, Hiroshi Masuda, and Masaki Aono. Watermarking three-dimensional polygonal models through geometric and topological modifications. *IEEE Journal on Selected Areas in Communications*, 16(4):551–560, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072138.html.

Ozaki:1993:HVP

[OMI93] S. Ozaki, T. Matsumoto, and H. Imai. A holder verification protocol using fingerprints. In Anonymous [Ano93g], pages 1–9. ISBN ???? LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/033159.html.

Omura:1990:PKC

[Omu90] J. Omura. A public key cell design for smart card chips. In ???? [???90], pages 983–985.

Ochi:1998:NSO

[OMV98] L. Satoru Ochi, N. Maculan, and R. M. Videira Figueiredo. A new self-organizing strategy based on elastic networks for solving the Euclidean traveling salesman problem. *Lecture Notes in Computer Science*, 1416:479–487, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

ONeil:1986:ETM

[O'N86] Patrick E. O'Neil. The Escrow transactional method. *ACM Transactions on Database Systems*, 11(4):405–430, December 1986. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL http://www.acm.org/pubs/articles/journals/tods/1986-11-4/p405-o_neil/p405-o_neil.pdf; http://www.acm.org/pubs/citations/journals/tods/1986-11-4/p405-o_neil/; http://www.acm.org/pubs/toc/Abstracts/tods/7265.html.

Ogawa:1998:WTM

[ONT98] Hiroshi Ogawa, Takao Nakamura, and Youichi Takashima. Watermark technique for motion pictures. *NTT R&D*, 47(6):715–718, 1998. CODEN NTTDEC. ISSN 0915-2326.

Okamoto:1990:DZKb

[OO90] Tatsuaki Okamoto and Kazuo Ohta. Disposable zero-knowledge authentications and their applications to untraceable electronic cash. *Lecture Notes in Computer Science*, 435: 481–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350481.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350481.pdf.

Ohta:1993:DMS

[OO93] Kazuo Ohta and Tatsuaki Okamoto. A digital multisignature scheme based on the Fiat–Shamir scheme. *Lecture Notes in Computer Science*, 739:139–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ohta:1998:CST

[OO98] K. Ohta and T. Okamoto. On concrete security treatment of signatures derived from identification. *Lecture Notes in Computer Science*, 1462:354–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ohta:1991:MAH

[OOK91] Kazuo Ohta, Tatsuaki Okamoto, and Kenji Koyama. Membership authentication for hierarchical multigroups using the extended Fiat–Shamir scheme. *Lecture Notes in Computer Science*, 473:446–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730446.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730446.pdf.

ORuanaidh:1997:RST

[OP97] Joseph J. K. O'Ruanaidh and Thierry Pun. Rotation, scale and translation invariant digital image watermarking. In IEEE [IEE97h], pages 536–539. ISBN 0-8186-8183-7, 0-8186-8184-5 (case). LCCN TK8315 .I16 1997. Three volumes. IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144.

ORuanaidh:1998:RST

[OP98] Joseph J. K. O'Ruanaidh and Thierry Pun. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 66(3):303–317, May 1998. CODEN SPRODR. ISSN 0165-1684. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073162.html.

ORuanaidh:1999:CCP

[ÓPH+99] Joseph Ó Ruanaidh, Holger Petersen, Alexander Herrigel, Shelby Pereira, and Thierry Pun. Cryptographic copyright protection for digital images based on watermarking techniques. *Theoretical Computer Science*, 226 (1–2):117–142, September 17, 1999. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1999&volume=226&issue=1-2&aid=3230`.

Oppliger:1996:ASS

[Opp96] Rolf Oppliger. *Authentication systems for secure networks*. The Artech House computer science library. Artech House Inc., Norwood, MA, USA, 1996. ISBN 0-89006-510-1. xvii + 186 pp. LCCN TK5105.59 .O77 1996. URL `http://www.artechhouse.com/Detail.aspx?strIsbn=978-0-89006-510-5`.

Oppliger:1997:ISF

[Opp97] Rolf Oppliger. Internet security: Firewalls and beyond. *Communications of the Association for Computing Machinery*, 40(5): 92–102, May 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/citations/journals/cacm/1997-40-5/p92-oppliger/`.

Otway:1987:ETM

[OR87] Dave Otway and Owen Rees. Efficient and timely mutual authentication. *Operating Systems Review*, 21(1):8–10, January 1987. CODEN OSRED8. ISSN 0163-5980.

OECD:1998:OEM

[Org98a] Organisation for Economic Co-operation and Computer Development. Committee for Information and Communications Policy. *OECD emerging market economy forum (EMEF): report of the workshop on cryptography, OECD, Paris, 9–10 December 1997*. Paris, France, 1998. 47 pp.

OECD:1998:CPG

[Org98b] Organisation for Economic Co-operation and Development. Ad hoc Group of Experts on Cryptography Policy Guidelines. *Cryptography policy: the guidelines and the issues*. Paris, France, 1998. 36 pp. Formulated by the Ad hoc Group of Experts on Cryptography Policy Guidelines.

Orlowski:1996:EGI

[Orl96] S. Orlowski. Encryption and the global information infrastructure: An Australian perspective. *Lecture Notes in Computer Science*, 1029:65–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Orton:1987:VIP

[ORS+87] G. A. Orton, M. P. Roy, P. A. Scott, L. E. Peppard, and S. E. Tavares. VLSI implementation of public-key encryption algorithms. In *Advances in cryptology—CRYPTO '86 (Santa Barbara, Calif., 1986)*, volume 263 of *Lecture Notes in Comput. Sci.*, pages 277–301. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987.

Orton:1995:MTD

[Ort95a] G. Orton. A multiple-iterated trapdoor for dense compact knapsacks. *Lecture Notes in Computer Science*, 950:112–130, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Orton:1995:MIT

[Ort95b] Glenn A. Orton. A multiple-iterated trapdoor for dense compact knapsacks. *Lecture Notes in Computer Science*, 950: 112–130, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500112.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500112.pdf`.

OShea:1988:CDU

[O'S88] G. O'Shea. Controlling the dependency of user access control mechanisms on correctness of user identification. *The Computer Journal*, 31(6):503–509, December 1988. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Okamoto:1991:EAC

[OS91] Tatsuaki Okamoto and Kouichi Sakurai. Efficient algorithms for the construction of hyperelliptic cryptosystems. *Lecture Notes in Computer Science*, 576: 267–278, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Okamoto:1992:EAC

[OS92] Tatsuaki Okamoto and Kouichi Sakurai. Efficient algorithms for the construction of hyperelliptic cryptosystems. *Lecture Notes* in *Computer Science*, 576: 267–278, 1992. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Olejar:1998:CPR

[OS98] D. Olejar and M. Stanek. On cryptographic properties of random Boolean functions. *J.UCS: Journal of Universal Computer Science*, 4(8):705–??, August 28, 1998. ISSN 0948-6968. URL `http://medoc.springer.de:8000/jucs/jucs_4_8/on_cryptographic_properties_of`.

Orup:1991:VER

[OSA91] Holger Orup, Erik Svendsen, and Erik Andreasen. VICTOR — an efficient RSA hardware implementation. *Lecture Notes in Computer Science*, 473: 245–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730245.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0473/04730245.pdf`.

Ong:1991:TCM

[OSH91] Sing Guat Ong, Jennifer Seberry, and Thomas. Hardjono. *Towards the cryptanalysis of Mandarin (Pinyin)*, volume 3 of *CCSR tutorial series in computer security*. Centre for Computer Security Research, Canberra, ACT, Australia, 1991. ISBN 0-7317-0177-1. ISSN 1034-1757. ix + 208 pp. LCCN ????

Ong:1985:ESS

[OSS85] H. Ong, C. P. Schnorr, and A. Shamir. Efficient signature schemes based on polynomial equations (preliminary version). In Blakley and Chaum [BC85], pages 37–46. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=37`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Okamoto:1998:NPK

[OU98a] Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as secure as factoring. *Lecture*

Notes in Computer Science, 1403:308–318, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030308.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030308.pdf.

Okamoto:1998:SIB

[OU98b] Tatsuaki Okamoto and Shigenori Uchiyama. Security of an identity-based cryptosystem and the related reductions. *Lecture Notes in Computer Science*, 1403:546–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030546.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030546.pdf.

Ou:1999:UUC

[Ou99] Y. Ou. On using UML class diagrams for object-oriented database design specification of integrity constraints. *Lecture Notes in Computer Science*, 1618: 173–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Outerbridge:1998:ACD

[Out98] Richard Outerbridge. AES candidate DEAL. In National Institute of Standards and Technology [Nat98], page 34. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf1/deal-slides.pdf. Only the slides for the conference talk are available.

Ozarow:1984:WTC

[OW84] Lawrence H. Ozarow and Aaron D. Wyner. Wire-tap channel II. *ATT Bell Lab. tech. j*, 63(10 part 1):2135–2157, 1984. CODEN ABLJER. ISSN 0748-612X (print), 2376-7162 (electronic).

OReilly:1995:WWW

[OW95] O'Reilly and Associates and Web Consortium (W3C), editors. *World Wide Web Journal: The Fourth International WWW Conference Proceedings*. 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, 1995. ISBN 1-56592-169-0. ISSN 1085-2301. LCCN TK5105.888 .I68 1995. US$39.95. URL http://www.ora.com/gnn/bus/ora/item/wj1.html. The World Wide Web Journal is a quarterly publication that provides timely, in-depth coverage of the issues, techniques, and research developments in the World Wide Web. The December issue contains the Conference Proceeding papers that were chosen for the 4th International World Wide Web conference in Boston, MA.

Ostrovsky:1991:HWM

[OY91] R. Ostrovsky and M. Yung. How to withstand mobile virus attacks. In *Proc. 10th ACM Symp. on Principles of Distributed Computation*, pages 51–61 (or 51–59??). ACM Press, New York, NY 10036, USA, 1991.

Pfitzmann:1993:MES

[PA93] Andreas Pfitzmann and Ralf Aßmann. More efficient software implementations of (generalized) DES. *Computers and Security*, 12(5):477–500, August 1993. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/016740489390069H`.

Pereira:1998:REC

[PA98a] R. Pereira and R. Adams. RFC 2451: The ESP CBC-Mode cipher algorithms, November 1998. URL `ftp://ftp.internic.net/rfc/rfc2451.txt`; `https://www.math.utah.edu/pub/rfc/rfc2451.txt`. Status: PROPOSED STANDARD.

Petitcolas:1998:WCM

[PA98b] F. A. P. Petitcolas and R. J. Anderson. Weaknesses of copyright marking systems. In Dittmann et al. [D+98], page ?? ISBN ???? LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/papers/acm98-weaknesses.doc`.

Paabo:1993:AD

[Pää93] Svante Pääbo. Ancient DNA. *Scientific American*, 269(5):86–?? (Intl. ed. 60–??), November 1993. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Padro:1998:RVS

[Pad98] Carles Padró. Robust vector space secret sharing schemes. *Information Processing Letters*, 68(3):107–111, November 15, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Pai:1996:VIE

[Pai96] Rajay R. Pai. VLSI implementation of the extended Data Encryption Standard algorithm. Thesis (M.S.), University of Texas at Arlington, Arlington, TX, USA, 1996. x + 85 pp.

Paillier:1998:INP

[Pai98a] P. Paillier. On ideal non-perfect secret sharing schemes. *Lecture Notes in Computer Science*, 1361: 207–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Paillier:1998:INS

[Pai98b] P. Paillier. On ideal non-perfect secret sharing schemes. *Lecture Notes in Computer Science*, 1361: 207–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Paillier:1999:EDF

[Pai99a] P. Paillier. Evaluating differential fault analysis of unknown cryptosystems. *Lecture Notes in Computer Science*, 1560: 235–244, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Paillier:1999:LCD

[Pai99b] P. Paillier. Low-cost double-size modular exponentiation or how to stretch your cryptoprocessor. *Lecture Notes in Computer Science*, 1560:223–234, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Paillier:1999:TPE

[Pai99c] P. Paillier. A trapdoor permutation equivalent to factoring. *Lecture Notes in Computer Science*, 1560: 219–222, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Paillier:1999:PKC

[Pai99d] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. *Lecture Notes in Computer Science*, 1592:223–238, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920223.htm; http://link.springer-ny.com/link/service/series/0558/papers/1592/15920223.pdf`.

Petitcolas:1998:ACM

[PAK98] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn. Attacks on copyright marking systems. In Aucsmith [Auc98], pages 219–239. ISBN 3-540-65386-4. LCCN QA76.9.A25I48 1998. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072113.html`.

Parthasarathy:1985:DSG

[Par85] Aiyaswamy Parthasarathy. Digital signature generator for cryptographic applications. Thesis (M.S.), South Dakota School of Mines and Technology, Rapid City, SD, USA, 1985. 148 pp.

Parker:1996:RCG

[Par96] Tom Parker. The role of cryptography in global communications. *Network Security*, 1996(5):13–17, May 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/1353485896819106`.

Parent:1998:ALM

[Par98a] Michael Parent. ActiveX licensing with MD5 encryption. *C/C++ Users Journal*, 16(12):??, December 1998. CODEN CCUJEX. ISSN 1075-2838.

Parker:1998:UMP

[Par98b] Frederick D. Parker. The unsolved messages of Pearl Harbor. In Deavours et al. [DKK+98], pages 57–75. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Parrish:1998:RMM

[Par98c] Edward A. Parrish. Report to members: Members react to privacy and encryption survey. *Computer*, 31(9):12–15, September 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co1998/pdf/r9012.pdf`.

Patterson:1987:MCC

[Pat87] Wayne Patterson. *Mathematical cryptology for computer scientists and mathematicians*. Rowman and Littlefield, Totowa, NJ, USA, 1987. ISBN 0-8476-7438-X. xxii + 312 pp. LCCN Z103 .P351 1987. US$29.50.

Patarin:1991:PPB

[Pat91a] J. Patarin. Pseudorandom permutations based on the DES scheme. *Lecture Notes in Computer Science*, 514: 193–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Patarin:1991:NRP

[Pat91b] Jacques Patarin. New results on pseudorandom permutation generators based on the DES scheme. *Lecture Notes in Computer Science*, 576:301–213, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Patarin:1995:CMI

[Pat95] Jacques Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88. *Lecture Notes in Computer Science*, 963:248–261, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630248.htm; http://link.springer-ny.com/link/service/series/0558/papers/0963/09630248.pdf.

Patarin:1996:ACH

[Pat96] J. Patarin. Asymmetric cryptography with a hidden monomial. *Lecture Notes in Computer Science*, 1109:45–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Paterson:1999:IPG

[Pat99] K. G. Paterson. Imprimitive permutation groups and trapdoors in iterated block ciphers. In Knudsen [Knu99c], pages 201–214. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Paulson:1998:IAV

[Pau98] Lawrence C. Paulson. *The inductive approach to verifying cryptographic protocols*. Technical report; no. 443. 4006797499. University of Cambridge Computer Laboratory, Cambridge, UK, USA, February 6, 1998. ii + 46 pp. LCCN QA76.9.A96 P3757 1998.

Paulson:1999:IAI

[Pau99] Lawrence C. Paulson. Inductive analysis of the Internet protocol TLS. *ACM Transactions on Information and System Security*, 2(3):332–351, August 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org/pubs/citations/journals/tissec/1999-2-3/p332-paulson/.

Poovendran:1999:ITA

[PB99a] R. Poovendran and J. S. Baras. An information theoretic analysis of rooted-tree based secure multicast key distribution schemes. In Wiener [Wie99], pages 624–638. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Proctor:1999:PC

[PB99b] Paul E. Proctor and Christian Byrnes. The politics of cryptography. *Performance Computing*, 17(11):25–29, October 1999. CODEN UNRED5. ISSN 0742-3136.

Piva:1997:DBW

[PBBC97] A. Piva, M. Barni, F. Bartolini, and V. Cappellini. DCT-based watermark recovering without resorting to the uncorrupted original image. In IEEE [IEE97h], pages 520–523. ISBN 0-8186-8183-7, 0-8186-8184-5 (case). LCCN TK8315 .I16 1997. Three volumes. IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144.

Preneel:1997:CHF

[PBD97] Bart Preneel, Antoon Bosselaers, and Hans Dobbertin. The cryptographic hash function RIPEMD-160. *CryptoBytes*, 3(2):9–14, Autumn 1997. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto3n2.pdf.

Preneel:1989:CHB

[PBGV89] Bart Preneel, Antoon Bosselaers, Rene Govaerts, and Joos Vandewalle. Collision-free hashfunctions based on blockcipher algorithms. In *Proceedings 1989 International Carnahan Conference on Security Technology (Oct 3–5 1989: Zurich, Switzerland)*, pages 203–210. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. IEEE catalog number 89CH2774-8.

Preneel:1990:CTA

[PBGV90] Bart Preneel, Antoon Bosselaers, René Govaerts, and Joos Vandewalle. A chosen text attack on the modified cryptographic checksum algorithm of Cohen and Huang. *Lecture Notes in Computer Science*, 435: 154–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350154.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350154.pdf.

Petrie:1998:NBR

[PC98] C. S. Petrie and J. A. Connelly. A noise-based random bit generator IC for applications in cryptography. In IEEE, editor, *ISCAS '98: proceedings of the 1998 IEEE International Symposium on Circuits and Systems: May 31–June 3, 1998, Monterey Conference Center, Monterey, CA*, volume 2. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN 0-7803-4455-3 (paperback), 0-7803-4456-1 (hardcover). LCCN TK7801.I22 1998.

Pizzonia:1999:OOD

[PD99a] M. Pizzonia and G. Di Battista. Object-oriented design of graph oriented data structures. *Lecture Notes in Computer Science*, 1619: 140–155, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Popovic:1999:DIT

[PD99b] D. Popovic and V. Devedzic. Designing an intelligent tutoring systems in the domain of formal languages. *Lecture Notes in Computer Science*, 1611:798–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Plagge:1999:DET

[PDGI99] M. Plagge, B. Diebold, R. Guenther, and J. Ihlenburg. Design and evaluation of the T-Team of the University of Tübingen for RoboCup'98. *Lecture Notes in Computer Science*, 1604:464–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pearcey:1980:EDS

[Pea80] T. (Trevor) Pearcey. *Encryption in data systems and communication*. Caulfield Institute of Technology. Computer Abuse Research and Bureau (CITCARB), Caulfield, Victoria, Australia, 1980. ISBN 0-909176-14-0. 99 pp. LCCN ????

Peake:1997:OVD

[Pea97] Hayden B. Peake. OSS and the Venona decrypts. *Intelligence and National Security*, 12(3):14–??, 1997. ISSN 0268-4527 (print), 1743-9019 (electronic).

Pedersen:1991:DPA

[Ped91a] T. P. Pedersen. Distributed provers with applications to undeniable signatures. In Davies [Dav91], pages 221–242. CODEN LNCSD9. ISBN 0-387-54620-0 (New York), 3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991. Rev. and expanded papers from the meeting which was sponsored by the International Association for Cryptology Research (IACR) and others.

Pedersen:1991:NIS

[Ped91b] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Feigenbaum [Fei91], pages 129–140. CODEN LNCSD9. ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1991.

URL http://link.springer-ny.com/link/service/series/0558/tocs/t0576.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=576. Conference held Aug. 11–15, 1991, at the University of California, Santa Barbara.

Pedersen:1991:TCT

[Ped91c] T. P. Pedersen. A threshold cryptosystem without a trusted party. In Davies [Dav91], pages 522–526. CODEN LNCSD9. ISBN 0-387-54620-0 (New York), 3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991. Rev. and expanded papers from the meeting which was sponsored by the International Association for Cryptology Research (IACR) and others.

Pedersen:1991:NII

[Ped91d] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. *Lecture Notes in Computer Science*, 576:129–140, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760129.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760129.pdf.

Pedersen:1991:NIT

[Ped91e] Torben Pryds Pedersen. Noninteractive and information-theoretic secure verifiable secret sharing. *Lecture Notes in Computer Science*, 576:129–140, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pedersen:1995:EPS

[Ped95] T. Pedersen. Electronic payments of small amounts. Technical Report DAIMI PB-495, Aarhus University, Computer Science Department, Aarhus, Denmark, August 1995.

Pedersen:1999:SCP

[Ped99] T. P. Pedersen. Signing contracts and paying electronically. *Lecture Notes in Computer Science*, 1561: 134–157, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pelta:1960:SP

[Pel60] Harold N. Pelta. Selfcipher: Programming. *Communications of the Association for Computing Machinery*, 3(2):83, February 1960. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Penzhorn:1996:CAS

[Pen96] W. T. Penzhorn. Correlation attacks on stream ciphers: Computing low-weight parity checks based on error-correcting codes. *Lecture Notes in Computer Science*, 1039:159–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Perret:1890:RCS

[Per90] P.-M. Perret. Les règles de Cicco Simonetta pour le déchiffrement des écritures secrètes (4 juillet 1474). (French) [the rules of Cicco Simonetta for decryption of secret writings (4 July 1474)]. *Bibliothèque de lÉcole des chartes*, 51: 516–525, 1890. ISSN 0373-6237 (print), 1953-8138 (electronic). URL `http://www.jstor.org/stable/43000437`.

Peralta:1985:TRN

[Per85] Rene Caupolican Peralta. *Three results in number theory and cryptography: a new algorithm to compute square roots modulo a prime number; On the bit complexity of the discrete logarithm; A framework for the study of cryptoprotocols*. Thesis (Ph.D.), Department of Computer Science, University of California, Berkeley, Berkeley, CA, USA, December 1985. 52 pp.

Perry:1988:EBG

[Per88] Tekla S. Perry. Electronic banking goes to market. *IEEE Spectrum*, 25(2):46–49, February 1988. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Perry:1991:EIT

[Per91] Chuckwudi Perry. An efficient implementation of triple enciphered Data Encryption Standard. Thesis (M.S.), Prairie View A and M University, Prairie View, TX 77446-2355, USA, 1991. xi + 67 pp.

Peralta:1993:QSD

[Per93] R. Peralta. A quadratic sieve on the n-dimensional cube. *Lecture Notes in Computer Science*, 740: 324–332, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Perrig:1997:CPE

[Per97] A. Perrig. *A Copyright Protection Environment for Digital Images*. Diploma dissertation, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, February 1997. ??–?? pp. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1052.html`.

Perkuhn:1999:DSC

[Per99] R. Perkuhn. Describing similar control flows for families of problem-solving methods. *Lecture Notes in Computer Science*, 1621: 361–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pesic:1997:SSS

[Pes97] Peter Pesic. Secrets, symbols, and systems: Parallels between cryptanalysis and algebra, 1580–1700. *Isis*, 88(4):674–692, December 1997. CODEN ISISA4. ISSN 0021-1753 (print), 1545-6994 (electronic). URL http://www.jstor.org/stable/237832.

Petho:1991:PTA

[Pet91] A. Pethö. On a polynomial transformation and its application to the construction of a public key cryptosystem. In *Computational number theory (Debrecen, 1989)*, pages 31–43. de Gruyter, Berlin, 1991.

Petersen:1998:HCD

[Pet98] H. Petersen. How to convert any digital signature scheme into a group signature scheme. *Lecture Notes in Computer Science*, 1361:177–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Panagopoulos:1994:BSS

[PF94] G. Panagopoulos and C. Faloutsos. Bit-sliced signature files for very large text databases on a parallel machine architecture. *Lecture Notes in Computer Science*, 779: 379–392, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pfitzmann:1995:BEA

[Pfi95] B. Pfitzmann. Breaking an efficient anonymous channel. *Lecture Notes in Computer Science*, 950:332–340 (or 339–348??), 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/032627.html.

Pfitzmann:1996:IHT

[Pfi96a] B. Pfitzmann. Information hiding terminology. In Anderson [And96c], pages 347–350. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054156.html.

Pfitzmann:1996:TTT

[Pfi96b] B. Pfitzmann. Trials of traced traitors. In Anderson [And96c], pages 49–64. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054622.html.

Pfitzmann:1996:DSS

[Pfi96c] Birgit Pfitzmann. *Digital signature schemes: general framework and fail-stop signatures*, volume 1100 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-61517-2 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). xvi + 396 pp. LCCN QA76.9.A25 P444 1996. Revision of thesis (Ph. D.)–University of Hildesheim, 1993.

Pfleeger:1989:SC

[Pfl89] Charles P. Pfleeger. *Security in computing*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1989. ISBN 0-13-798943-1. xxi + 538 pp. LCCN QA76.9.A25 P45 1989.

Pfleeger:1995:ULC

[Pfl95] Charles Pfleeger. Uncryptic look at cryptography. *IEEE Software*, 12(1):121–123, January 1995. CODEN IESOEG. ISSN 0740-7459 (print), 1937-4194 (electronic). Review of Bruce Schneier's *Applied Cryptography*.

Pfleeger:1997:SC

[Pfl97] Charles P. Pfleeger. *Security in computing*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, second edition, 1997. ISBN 0-13-337486-6. xviii + 574 pp. LCCN QA76.9.A25 P45 1997.

Pomerance:1990:CCNb

[PG90] Carl Pomerance and S. Goldwasser, editors. *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of symposia in applied mathematics. AMS short course lecture notes.* American Mathematical Society, Providence, RI, USA, 1990. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

Patarin:1997:ACB

[PG97a] J. Patarin and L. Goubin. Asymmetric cryptography with S-boxes. *Lecture Notes in Computer Science*, 1334: 369–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Patarin:1997:ACS

[PG97b] J. Patarin and L. Goubin. Asymmetric cryptography with S-boxes. *Lecture Notes in Computer Science*, 1334: 369–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pieprzyk:1996:CBT

[PGCSN96] J. Pieprzyk, H. Ghodosi, C. Charnes, and R. Safavi-Naini. Cryptography based on transcendental numbers. *Lecture Notes in Computer Science*, 1172:96–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1991:CRH

[PGV91] B. Preneel, R. Govaerts, and J. Vandewalle. Collision resistant hash functions based on blockciphers. In Feigenbaum [Fei91], page ?? CODEN LNCSD9. ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1991. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0576.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=576`. Conference held Aug. 11–15, 1991, at the University of California, Santa Barbara.

Preneel:1992:CSH

[PGV92] B. Preneel, R. Govaerts, and J. Vandewalle. Cryptographically secure hash functions: an overview. In *????*, page ?? ????, ????, 1992. Reference in [PS93b, p. 186].

Preneel:1993:CHF

[PGV93a] B. Preneel, R. Govaerts, and J. Vandewalle. Cryptographic hash functions. In Wolfowicz [Wol93b], pages 161–171. LCCN ????

Preneel:1993:HFB

[PGV93b] B. Preneel, R. Govaerts, and J. Vandewalle. Hash functions based on block ciphers: a synthetic approach. In Stinson [Sti93b], pages 368–378. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). LCCN QA76.9.A25 C79 1993.

Preneel:1993:IAH

[PGV93c] B. Preneel, R. Govaerts, and J. Vandewalle. Information authentication:

Hash functions and digital signatures. *Lecture Notes in Computer Science*, 741: 87–131, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1993:CSI

[PGV93d] Bart Preneel, Rene Govaerts, and J. Vandewalle, editors. *Computer security and industrial cryptography: state of the art and evolution: ESAT course, Leuven, Belgium, May 21–23, 1991*, volume 741 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. CODEN LNCSD9. ISBN 0-387-57341-0 (U.S.). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C6373 1993. DM58.00.

Preneel:1994:HFB

[PGV94] Bart Preneel, Rene Govaerts, and Joos Vandewalle. Hash functions based on block ciphers: a synthetic approach. *Lecture Notes in Computer Science*, 773: 368–378, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pohlig:1978:IAC

[PH78] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 24 (1):106–111, ???? 1978. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Post:1991:RSE

[PH91] Frits H. Post and Andrea J. S. Hin. Report on the Second Eurographics Workshop on Visualization in Scientific Computing. *Computer Graphics Forum*, 10(3): 261–264, September 1991. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Praun:1999:RMW

[PHF99] Emil Praun, Hugues Hoppe, and Adam Finkelstein. Robust mesh watermarking. *Computer Graphics*, 33 (Annual Conference Series): 49–56, 1999. CODEN CGRADI, CPGPBZ. ISSN 0097-8930 (print), 1558-4569 (electronic). URL `http://www.acm.org/pubs/citations/proceedings/graph/311535/p49-praun/`.

Phillips:1998:SHI

[Phi98] Dwayne Phillips. Steganography: Hiding information in plain sight. *C/C++ Users Journal*, 16(11):49–??, November 1998. CO-

DEN CCUJEX. ISSN 1075-2838.

Pichler:1986:ACE

[Pic86] Franz Pichler, editor. *Advances in cryptology: Eurocrypt 85: proceedings of a workshop on the theory and application of cryptographic techniques, Linz, Austria, April, 1985*, volume 219 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1986. CODEN LNCSD9. ISBN 0-387-16468-5 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E961 1985. "The workshop was sponsored by International Association for Cryptologic Research ... [et al.]"–T.p. verso.

Pichler:1998:E

[Pic98] F. Pichler. EUROCRYPT '85. *Lecture Notes in Computer Science*, 1440:41–48, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pierce:1977:SSP

[Pie77] Clayton C. Pierce. *Secret and secure: privacy, cryptography, and secure communication*. Pierce, Ventura, CA, USA, 1977. iv + 84 pp. LCCN Z103.P531.

Pieper:1993:CRD

[Pie93] Reinhold Pieper. Cryptanalysis of Rédi- and Dickson permutations on arbitrary finite rings. *Applicable algebra in engineering, communication and computing*, 4(1):59–76, 1993. CODEN AAECEW. ISSN 0938-1279 (print), 1432-0622 (electronic).

Pinch:1997:UCN

[Pin97] R. G. E. Pinch. On using Carmichael numbers for public key encryption systems. *Lecture Notes in Computer Science*, 1355: 265–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Piner:1998:CUW

[Pin98] Mary-Louise G. Piner. CS update; WW II cryptologist [Jack Good] receives Pioneer Award; Colossus builder Tommy Flowers (1905–1998); DCI founder [George Schussel] receives Entrepreneur Award; 1998 Bell Prize recognizes advances in parallel processing. *Computer*, 31(12):70–73, December 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co1998/pdf/rz070.pdf`.

Pitas:1995:PIW

[Pit95] I. (Ioannis) Pitas, editor. *Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing (Neos Marmaras, Halkidiki, Greece, June 20–22, 1995)*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1995. LCCN ???? Two volumes.

Pitas:1996:MSC

[Pit96a] I. Pitas. A method for signature casting on digital images. In IEEE [IEE96e], pages 215–218. ISBN 0-7803-3258-X (softbound), 0-7803-3259-8 (casebound), 0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM). LCCN TK8315.I222 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/063160.html`. Three volumes. IEEE catalog number 96CH35919.

Pitoura:1996:RSS

[Pit96b] E. Pitoura. A replication schema to support weak connectivity in mobile information systems. *Lecture Notes in Computer Science*, 1134:510–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Price:1999:IAV

[PJ99] A. R. Price and T. Jones. An innovative approach to vision, localization and orientation using omnidirectional radial signature analysis. *Lecture Notes in Computer Science*, 1604:299–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Panneerselvam:1990:RSA

[PJBM90] G. Panneerselvam, G. A. Jullien, S. Bandyopadhyay, and W. C. Miller. Reconfigurable systolic architectures for hashing. In *Proceedings — Parbase-90 International Conference on Databases, Parallel Architectures, and Their Applications (Mar 7–9 1990: Miami Beach, FL, USA)*, pages 543–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. IEEE catalog number 90CH2728-4.

Popek:1979:ESC

[PK79] Gerald J. Popek and Charles S. Kline. Encryption and secure computer networks. *ACM Computing Surveys*, 11(4):331–356, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Penzhorn:1995:CLP

[PK95a] W. T. Penzhorn and G. J. Kuehn. Computation of low-weight parity checks for correlation attacks on stream ciphers. *Lecture*

Notes in Computer Science, 1025:74–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Penzhorn:1995:CLW

[PK95b] W. T. Penzhorn and G. J. Kuehn. Computation of low-weight parity checks for correlation attacks on stream ciphers. *Lecture Notes in Computer Science*, 1025:74–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Praehofer:1999:SRS

[PK99] H. Praehofer and J. Kerschbaummayr. Supporting reusability in a system design environment by case-based reasoning techniques. *Lecture Notes in Computer Science*, 1650:535–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pamplona:1998:LVC

[PKA+98] August Pamplona, Mike Kurtinitis, Stuart Ambler, Win Carus, Tim McCaffrey, and Peter Sage. Letters: Visual cryptography; Ecco-Fan; help wanted; ternary searches; window sizes and the registry. *Dr. Dobb's Journal of Software Tools*, 23(6):10, 12, June 1998. CODEN DDJOEB. ISSN 1044-789X.

Postma:1997:DCF

[PKM97] A. Postma, T. Krol, and E. Molenkamp. Distributed cryptographic function application protocols. *Lecture Notes in Computer Science*, 1334:435–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Park:1994:KDA

[PKOT94] Choonsik Park, Kaoru Kurosawa, Tatsuaki Okamoto, and Shigeo Tsujii. On key distribution and authentication in mobile radio networks. *Lecture Notes in Computer Science*, 765: 461–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650461.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650461.pdf`.

Petrounias:1994:RBA

[PL94] I. Petrounias and P. Loucopoulos. A rule-based approach for the design and implementation of information systems. *Lecture Notes in Computer Science*, 779: 159–172, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pless:1975:ESC

[Ple75] Vera Pless. Encryption schemes for computer confidentially [sic]. MAC technical memorandum 63, Massachusetts Institute of Technology, Project MAC, Cambridge, MA, USA, 1975. 19 pp. Research done under ARPA Order no.2095, ONR Contract no. N00014-70-A-0362-0006 and IBM Contract 82280.

Pless:1977:ESC

[Ple77] Vera S. Pless. Encryption schemes for computer confidentiality. *IEEE Transactions on Computers*, C-26 (11):1133–1136, 1977. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Plimmer:1998:MIW

[Pli98] Beryl Plimmer. Machines invented for WW II code breaking. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 30(4):37–40, December 1998. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Plumstead:1982:ISG

[Plu82] Joan Boyar Plumstead. Inferring a sequence generated by a linear congruence. In IEEE [IEE82a], pages 153–159. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

Plumstead:1983:ISP

[Plu83] Joan Boyar Plumstead. *Inferring Sequences Produced by Pseudo-Random Number Generators*. Ph.D. dissertation, Department of Computer Science, University of California, Berkeley, Berkeley, CA, USA, June 1983. ii + 56 pp.

Pei:1999:COA

[PLWSN99] Dingyi Pei, Yuqiang Li, Yejing Wang, and Rei Safavi-Naini. Characterization of optimal authentication codes with arbitration. *Lecture Notes in Computer Science*, 1587: 303–313, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1587/15870303.htm; http://link.springer-ny.com/link/service/series/0558/papers/1587/15870303.pdf`.

Payne:1978:OEN

[PM78] W. H. Payne and K. L. McMillen. Orderly enumeration of nonsingular binary matrices applied to text encryption. *Communications of the Association* *for Computing Machinery*, 21(4):259–263, April 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Petersen:1998:SST

[PM98] H. Petersen and M. Michels. On signature schemes with threshold verification detecting malicious verifiers. *Lecture Notes in Computer Science*, 1361:67–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pitt:1999:DAC

[PM99a] J. Pitt and A. Mamdani. Designing agent communication languages for multi-agent systems. *Lecture Notes in Computer Science*, 1647:102–114, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Provos:1999:FAP

[PM99b] Niels Provos and David Mazieres. A future-adaptable password scheme. In USENIX [USE99d], page ?? ISBN 1-880446-33-2. LCCN ???? URL `http://www.openbsd.org/papers/bcrypt-paper.ps`.

Prie:1999:ASU

[PMP99] Y. Prie, A. Mille, and J.-M. Pinon. AI-STRATA: a user-centered model for content-based description and retrieval of audiovisual sequences. *Lecture Notes in Computer Science*, 1554: 328–343, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Proctor:1992:AIC

[PN92] N. Proctor and P. Neumann. Architectural implications of covert channels. In NIST [NIS92], pages 28–43. LCCN QA76.9.A25 N38 1992. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/021136.html`. Two volumes.

Pudil:1995:ASM

[PNFK95] P. Pudil, J. Novovicova, F. Ferri, and J. Kittler. Advances in the statistical methodology for the selection of image descriptors for visual pattern representation and classification. *Lecture Notes in Computer Science*, 970:832–837, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1994:CCM

[PNRB94] Bart Preneel, Marnix Nuttin, Vincent Rijmen, and Johan Buelens. Cryptanalysis of the CFB mode of the DES with a reduced number of rounds. *Lecture Notes in Computer Science*, 773:212–??, 1994. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pointcheval:1999:NPK

[Poi99] David Pointcheval. New public key cryptosystems based on the dependent — RSA problems. *Lecture Notes in Computer Science*, 1592:239–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1592/15920239.htm; http://link.springer-ny.com/link/service/series/0558/papers/1592/15920239.pdf`.

Pollard:1974:TFP

[Pol74] J. Pollard. Theorems on factorization and primality testing. *Proceedings of the Cambridge Philosophical Society. Mathematical and physical sciences*, 76: 521–528, 1974. CODEN PCPSA4. ISSN 0008-1981.

Pollard:1978:MCM

[Pol78] J. M. Pollard. Monte Carlo methods for index computation $(\bmod p)$. *Mathematics of Computation*, 32 (143):918–924, July 1978. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Pomerance:1988:ACC

[Pom88] Carl Pomerance, editor. *Advances in cryptology — CRYPTO '87: proceedings*, volume 293 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-18796-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1987; QA267.A1 L43 no.293. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0293.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=293`. CRYPTO '87, a Conference on the Theory and Applications of Cryptographic Techniques, held at the University of California, Santa Barbara ... August 16–20, 1987.

Pomerance:1990:CCNa

[Pom90a] Carl Pomerance. Cryptology and computational number theory — an introduction. In Pomerance and Goldwasser [PG90], pages 1–12. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

Pomerance:1990:F

[Pom90b] Carl Pomerance. Factoring. In Pomerance and Goldwasser [PG90], pages 27–47. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

Pomerance:1994:NFS

[Pom94] C. Pomerance. The number field sieve. In W. Gautschi, editor, *Mathematics of Computation 1943–1993: A Half-Century of Computational Mathematics. Mathematics of Computation 50th Anniversary Symposium, August 9–13, 1993, Vancouver, British Columbia*, volume 48 of *Proceedings of symposia in applied mathematics*, pages 465–480. American Mathematical Society, Providence, RI, USA, 1994. ISBN 0-8218-0291-7, 0-8218-0353-0 (pt. 1), 0-8218-0354-9 (pt. 2). LCCN QA1 .A56 v.48 1994.

Pomerance:1998:C

[Pom98] C. Pomerance. Crypto '87. *Lecture Notes in Computer Science*, 1440:75–80, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ponting:1989:TCB

[Pon89] Bob Ponting. Three companies break Adobe encryption scheme. *InfoWorld*, 11(9):8, February 2, 1989. CODEN INWODU. ISSN 0199-6649. URL https://books.google.com/books?id=IToEAAAAMBAJ&pg=PT7.

Poole:1995:La

[Poo95] Gary Andrew Poole. Logout. *Open Computing*, 12 (1):112–??, January 1995. CODEN OPCOEB. ISSN 1078-2370.

Popentiu:1989:SRK

[Pop89] Fl. Popenţiu. A survey of recent knapsack cryptosystems. *Bul. Inst. Politehn. Bucureşti Ser. Electron.*, 51: 83–90, 1989.

Pope:1996:PF

[Pop96] Trevor J. Pope. Password files. *Dr. Dobb's Journal of Software Tools*, 21 (1):72, 74, 76, 101, 103–104, January 1996. CODEN DDJOEB. ISSN 1044-789X.

Porges:1952:MNC

[Por52] Arthur Porges. Mathematical notes: a continued fraction cipher. *American Mathematical Monthly*, 59

(4):236, April 1952. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Porter:1984:CNS

[Por84] Sig Porter. Cryptology and number sequences: Pseudorandom, random, and perfectly random. *Computers and Security*, 3(1):43–44, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900257`.

Portz:1991:UIN

[Por91] M. Portz. On the use of interconnection networks in cryptography. *Lecture Notes in Computer Science*, 547:302–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Portz:1993:GDB

[Por93] M. Portz. A generalized description of DES-based and Benes-based permutation generators. *Lecture Notes in Computer Science*, 718:397–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Poromaa:1998:PAT

[Por98] P. Poromaa. Parallel algorithms for triangular Sylvester equations: Design, scheduling and sealability issues. *Lecture Notes in Computer Science*, 1541: 438–446, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Posch:1992:TMD

[Pos92] Reinhard Posch. Trustworthy management of distribution and operation of encryption devices. Report 344, Institutes for Information Processing, Graz, Austria, October 1992. 11 + 3 pp.

Posch:1993:PFP

[Pos93] Reinhard Posch. Pipelining and full parallelism for long integer arithmetic in encryption devices. Report 357, Institutes for Information Processing Graz, Graz, Austria, March 1993. 8 pp.

Posch:1998:MPC

[Pos98] Reinhard Posch. Massive parallelism on a chip: VLSI aspects involving dynamic logic. *International Journal of Computer Systems Science and Engineering*, 13 (2):101–107, March 1998. CODEN CSSEEI. ISSN 0267-6192.

Posch:1989:AEA

[PP89] K. C. Posch and R. Posch. Approaching encryption at ISDN speed using partial parallel modulus multiplication. IIG report 276, Institutes for Information Processing Graz, Graz, Austria, November 1989. 9 pp.

Pfitzmann:1990:HBD

[PP90] B. Pfitzmann and A. Pfitzmann. How to break the direct RSA-implementation of MIXes. In Quisquater and Vandewalle [QV90], pages 373–?? CODEN LNCSD9. ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1989; QA267.A1 L43 no.434. DM98.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340373.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340373.pdf; http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1023.html.

Posch:1992:MRR

[PP92a] K. C. Posch and R. Posch. Modulo reduction in residue number systems. Technical report, Inst., TU, Ges., ????, 1992. 16 pp. URL http://books.google.com/books?id=YPLKHAAACAAJ.

Posch:1992:RNS

[PP92b] K. C. Posch and R. Posch. Residue number systems: a key to parallelism in public key cryptography. In *Proceedings of the Fourth IEEE Symposium on Parallel and Distributed Processing 1992*, pages 432–435. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. CODEN ???? ISSN ????

Posch:1995:MRRb

[PP95a] K. C. Posch and R. Posch. Modulo reduction in residue number systems. *IEEE Transactions on Parallel and Distributed Systems*, 6(5):449–454, May 1995. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=8666.

Posch:1995:MRRa

[PP95b] Karl C. Posch and Reinhard Posch. Modulo reduction in residue number systems. *IEEE Transactions on Parallel and Distributed Systems*, 6(5):449–454, May 1995. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Pakstas:1996:SNN

[PP96] Algirdas Pakstas and Sonata Pakstiene. Standards: NSK: A Norwegian cryptochip for supersafe communications. *Computer*, 29 (2):78–79, February 1996. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Pedersen:1997:FSS

[PP97] Torben Pryds Pedersen and Birgit Pfitzmann. Fail-stop signatures. *SIAM Journal on Computing*, 26(2):291–330, April 1997. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/toc/SICOMP/26/2`.

Park:1997:TER

[PPKW97] Sangjoon Park, Sangwoo Park, Kwangjo Kim, and Dongho Won. Two efficient RSA multisignature schemes. *Lecture Notes in Computer Science*, 1334: 217–222, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Peleg:1979:BSC

[PR79] Shmuel Peleg and Azriel Rosenfeld. Breaking substitution ciphers using a relaxation algorithm. *Communications of the Association for Computing Machinery*, 22(11):598–605, November 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Pieprzyk:1985:DPK

[PR85a] Józef P. Pieprzyk and Dominik A. Rutkowski. Design of public key cryptosystems using idempotent elements. *Computers and Security*, 4(4):297–308, December 1985. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404885900483`.

Pieprzyk:1985:MDI

[PR85b] Józef P. Pieprzyk and Dominik A. Rutkowski. Modular design of information encipherment for computer systems. *Computers and Security*, 4(3):211–218, September 1985. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404885900306`.

Preneel:1998:SAA

[PR98] Bart Preneel and Vincent Rijmen, editors. *State of the art in applied cryptography: course on computer security and industrial cryptography, Leuven, Belgium, June 3–6, 1997: revised lectures*, volume 1528 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-65474-7 (paperback).

LCCN QA76.9.A25S735 1998.

Pratt:1939:SUS

[Pra39] Fletcher Pratt. *Secret and urgent: the story of codes and ciphers*. Robert Hale, London, UK, 1939. 282 pp. LCCN Z104 .P92 1939.

Pratt:1996:SUS

[Pra96] Fletcher Pratt. *Secret and Urgent: the Story of Codes and Ciphers*, volume 72 of *Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1996. ISBN 0-89412-261-4 (paperback). 282 pp. LCCN Z104 .P92 1996.

Parra:1998:MPS

[PRAM98] A. Parra, M. Rincon, J. R. Alvarez, and J. Mira. A modular and parametric structure for the substitution redesign of power plants control systems. *Lecture Notes in Computer Science*, 1416:896–906, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1998:RDD

[PRB98a] B. Preneel, V. Rijmen, and A. Bosselaers. Recent developments in the design of conventional cryptographic algorithms. *Lecture Notes in Computer Science*, 1528: 105–130, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1998:AAP

[PRB98b] Bart Preneel, Vincent Rijmen, and Antoon Bosselaers. Algorithm alley: Principles and performance of cryptographic algorithms. *Dr. Dobb's Journal of Software Tools*, 23(12):126–131, December 1998. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ddj/1998/1998_12/shas/shas.htm`.

Preneel:1993:ADC

[Pre93a] B. Preneel. *Analysis and Design of Cryptographic Hash Functions*. Thesis (Ph.D.), Katholieke Universiteit Leuven, Leuven, Belgium, January 1993. 355 pp. URL `http://wwwlib.umi.com/dissertations/fullcit/f64276`.

Preneel:1993:SCT

[Pre93b] B. Preneel. Standardization of cryptographic techniques. *Lecture Notes in Computer Science*, 741: 162–173, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1994:CHF

[Pre94a] Bart Preneel. Cryptographic hash functions. *European transactions on* *telecommunications and related technologies*, 5(4):431–448, 1994. CODEN ETTTET. ISSN 1120-3862.

Prenel:1994:CHF

[Pre94b] B. Prenel. Cryptographic hash functions. *European transactions on telecommunications and related technologies*, 5(4):431–??, July 1, 1994. CODEN ETTTET. ISSN 1120-3862.

Preneel:1995:FSE

[Pre95a] Bart Preneel, editor. *Fast software encryption: second international workshop, Leuven, Belgium, December 14–16, 1994: proceedings*, volume 1008 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-60590-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F37 1995.

Preneel:1995:EFC

[Pre95b] Bart Preneel. To the Editor: Further comments on keyed MD5. *CryptoBytes*, 1 (2):15, Summer 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf.

Preneel:1997:HFM

[Pre97a] B. Preneel. Hash functions and MAC algorithms based on block ciphers. *Lecture Notes in Computer Science*, 1355:270–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

PGP:1997:PGPa

[Pre97b] Pretty Good Privacy, Inc. *Pretty Good Privacy PGP-mail 4.5 program: quick guide*. Pretty Good Privacy, Inc., San Mateo, CA, USA, 1997. ISBN 0-9649654-3-7. iv + 34 pp. LCCN ????

PGP:1997:PGPb

[Pre97c] Pretty Good Privacy, Inc. *Pretty Good Privacy PGP-mail 4.5 program: reference manual*. Pretty Good Privacy, Inc., San Mateo, CA, USA, 1997. ISBN 0-9649654-4-5. xiv + 202 pp. LCCN ????

Preneel:1998:CMA

[Pre98a] B. Preneel. Cryptanalysis of message authentication codes. *Lecture Notes in Computer Science*, 1396: 55–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1998:IC

[Pre98b] B. Preneel. An introduction to cryptology. *Lecture Notes in Computer Science*, 1521:204–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1998:CPI

[Pre98c] Bart Preneel. Cryptographic primitives for information authentication — state of the art. *Lecture Notes in Computer Science*, 1528:49–104, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1528/15280049.htm; http://link.springer-ny.com/link/service/series/0558/papers/1528/15280049.pdf.

Preneel:1999:SCH

[Pre99] B. Preneel. The state of cryptographic hash functions. *Lecture Notes in Computer Science*, 1561: 158–182, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pritchard:1980:DE

[Pri80] John Arthur Thomas (John A. T.) Pritchard. *Data encryption*. National Computing Centre, Manchester, UK, 1980. ISBN 0-85012-253-8. 126 (or 118??) pp. LCCN QA76.9.A25 P7.

Price:1983:ABR

[Pri83] W. L. Price. *Annotated bibliography of recent publications on data security and cryptography*, volume 35/83 of *NPL-DITC*. National Physical Laboratory, Teddington, Middlesex, UK, sixth edition, 1983. ii + 29 pp. LCCN Z103.A1 P74 1983a. Reprinted by permission of the Controller of Her Britannic Majesty's Stationery Office. "PB84-169168." Photocopy. Springfield, VA: National Technical Information Service, [1983?]. 28 cm.

Price:1994:MVC

[Pri94] D. Price. Micro view. clipper: soon a de facto standard? *IEEE Micro*, 14 (4):80–80, 79, July/August 1994. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Pronzini:1980:MCC

[Pro80] Bill Pronzini. *Mummy!: a chrestomathy of crypt-ology*. Arbor House, New York, NY, USA, 1980. ISBN 0-87795-271-X. xii + 273 pp. LCCN PN 6120.95 M77 M86 1980. US$10.95. Contents: Doyle, A.C. Lot no. 249.–Poe, E.A. Some words with a mummy.–Benson, E.F. Monkeys.–Wollheim, D.A. Bones.–Williams, T. The vengeance of Nitocris.–Gautier, T. The mummy's foot.–Bloch, R. The eyes of the mummy.–Powell, T. Charlie.–Hoch, E.D. The weekend magus.–Lansdale, J.R. The princess.–Mayhar,

A. The eagle-claw rattle.–Grant, C.L. The other room.–Malzberg, B.N. Revelation in seven stages.–Bibliography.

Proctor:1985:SSC

[Pro85] Norman Proctor. A self-synchronizing cascaded cipher system with dynamic control of error propagation. In Blakley and Chaum [BC85], pages 174–190. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=174`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Patel:1999:TML

[PRS99] S. Patel, Z. Ramzan, and G. S. Sundaram. Towards making Luby-Rackoff ciphers optimal and practical. In Knudsen [Knu99c], pages 171–185. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Peyravian:1999:HBE

[PRZ99] M. Peyravian, A. Roginsky, and N. Zunic. Hash-based encryption system. *Computers and Security*, 18(4): 345–350, 1999. CODEN CPSEDU. ISSN 0167-4048.

Paun:1993:CPS

[PS93a] Gheorghe Păun and Arto Salomaa. Closure properties of slender languages. *Theoretical Computer Science*, 120(2):293–301, November 22, 1993. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1993&volume=120&issue=2&aid=1406`.

Pieprzyk:1993:DHA

[PS93b] Josef Pieprzyk and Babak Sadeghiyan. *Design of Hashing Algorithms*, volume 756 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-57500-6 (New York), 3-540-57500-6 (Berlin). xiii + 194 pp. LCCN QA76.9.H36 P53 1993.

Pfitzmann:1996:AF

[PS96a] B. Pfitzmann and M. Schunter. Asymmetric fingerprinting. In Maurer [Mau96b], pages

84–95. CODEN LNCSD9. ISBN 3-540-61186-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/053630.html. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Pichler:1996:FDG

[PS96b] F. Pichler and J. Scharinger. Finite dimensional generalized Baker dynamical systems for cryptographic applications. *Lecture Notes in Computer Science*, 1030: 465–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pointcheval:1996:PSB

[PS96c] D. Pointcheval and J. Stern. Provably secure blind signature schemes. *Lecture Notes in Computer Science*, 1163:252–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pointcheval:1996:SPS

[PS96d] D. Pointcheval and J. Stern. Security proofs for signature schemes. *Lecture Notes in Computer Science*, 1070: 387–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Parker:1997:GFA

[PS97] M. G. Parker and S. J. Shepherd. The generation of finite alphabet codewords with no cyclic shift or reversal symmetry. In ????, editor, *Proceedings of the 4th International Symposium on Communications Theory and Applications, 13–18 July 1997, Ambleside, The English Lakes*, page ?? ????, ????, 1997. ISBN ???? LCCN ????

Padro:1998:SSS

[PS98a] C. Padro and G. Saez. Secret sharing schemes with bipartite access structure. *Lecture Notes in Computer Science*, 1403:500–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Patel:1998:EDL

[PS98b] S. Patel and G. S. Sundaram. An efficient discrete log pseudo random generator. *Lecture Notes in Computer Science*, 1462: 304–317, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073818.html.

Patiyoot:1998:APW

[PS98c] D. Patiyoot and S. J. Shepherd. Authentication protocols for Wireless ATM networks. In ????, editor, *Proceedings of IEEE ICATM '98, (1) 22–24 June 1998, Colmar, France*, pages 87–96. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN ???? LCCN ????

Patiyoot:1998:SIW

[PS98d] D. Patiyoot and S. J. Shepherd. Security issues for wireless ATM networks. In ????, editor, *Proceedings of IEEE ICUPC '98, (2), 5-9 October 1998, Florence, Italy*, pages 1359–1363. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN ???? LCCN ????

Patiyoot:1998:TAPa

[PS98e] D. Patiyoot and S. J. Shepherd. Techniques for authentication protocols and key distribution on wireless ATM networks. *Operating Systems Review*, 32(4):25–32, October 1998. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Patiyoot:1998:TAPb

[PS98f] D. Patiyoot and S. J. Shepherd. Techniques for authentication protocols and key management for Wireless ATM networks. In ????, editor, *Proceedings of IEEE ICT '98, (4) 21-25 June 1998, Porto Carras, Greece*, pages 423–427. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN ???? LCCN ????

Poupard:1998:GSR

[PS98g] G. Poupard and J. Stern. Generation of shared RSA keys by two parties. *Lecture Notes in Computer Science*, 1514:11–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Poupard:1998:SAP

[PS98h] Guillaume Poupard and Jacques Stern. Security analysis of a practical "on the fly" authentication and signature generation. *Lecture Notes in Computer Science*, 1403: 422–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030422.htm; http://link.springer-ny.com/link/service/series/`

0558/papers/1403/14030422.pdf.

Patiyoot:1999:MES

[PS99a] D. Patiyoot and S. J. Shepherd. Modelling and evaluation of security induced delay in wireless ATM networks. *Operating Systems Review*, 33(3):26–31, July 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Patiyoot:1999:WSS

[PS99b] D. Patiyoot and S. J. Shepherd. WASS: a security services for wireless ATM networks. *Operating Systems Review*, 33(4):36–41, October 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Patiyoot:1999:SIA

[PS99c] Danai Patiyoot and S. J. Shepard. Security issues in ATM networks. *Operating Systems Review*, 33(4):22–35, October 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Patiyoot:1999:CST

[PS99d] Danai Patiyoot and S. J. Shepherd. Cryptographic security techniques for wireless networks. *Operating Systems Review*, 33(2):36–50, April 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Patiyoot:1999:WWA

[PS99e] Danai Patiyoot and S. J. Shepherd. WASS: wireless ATM security system. *Operating Systems Review*, 33 (2):29–35, April 1999. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Pfenning:1999:SDT

[PS99f] F. Pfenning and C. Schuermann. System description: Twelf — a meta-logical framework for deductive systems. *Lecture Notes in Computer Science*, 1632:202–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Patel:1997:UDB

[PSB97] A. Patel, N. Schmidt, and M. Bessonov. Using datagram based multimedia streams as a cover channel for hidden transmission. In Katsikas [Kat97], pages 239–249. ISBN 0-412-81770-5. LCCN QA76.9.A25 I464 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064168.html.

Pieprzyk:1991:RAS

[PSN91] Józef P. Pieprzyk and Reihaneh Safavi-Naini. Randomized authentication systems. *Lecture Notes in Computer Science*, 547: 472–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470472.htm; http://link.springer-ny.com/link/service/series/0558/papers/0547/05470472.pdf.

Pieprzyk:1995:PA

[PSN95a] J. Pieprzyk and R. Safavi-Naini, editors. *Proceedings — ASIACRYPT '94*, volume 917 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995.

Pieprzyk:1995:ACA

[PSN95b] Josef Pieprzyk and Reihanah Safavi-Naini, editors. *Advances in cryptology, ASIACRYPT '94: 4th International Conference on the Theory and Application of Cryptology, Wollongong, Australia, November 28–December 1, 1994: proceedings*, volume 917 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-59339-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 1994. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0917.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=917.

Paar:1997:FAA

[PSR97] Christof Paar and Pedro Soria-Rodriguez. Fast arithmetic architectures for public-key algorithms over Galois fields $GF((2^n)^m)$. *Lecture Notes in Computer Science*, 1233:363–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330363.htm; http://link.springer-ny.com/link/service/series/0558/papers/1233/12330363.pdf.

Pomerance:1988:PAF

[PST88] Carl Pomerance, J. W. Smith, and Randy Tuler. A pipeline architecture for factoring large integers with the quadratic sieve algorithm. *SIAM Journal on Computing*, 17(2):387–403, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Pomerance:1980:P

[PSW80] Carl Pomerance, J. L. Selfridge, and Samuel S. Wagstaff, Jr. The pseudoprimes to $25 \cdot 10^9$. *Mathematics of Computation*, 35 (151):1003–1026, July 1980. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Pfitzmann:1995:HBA

[PSW95] B. Pfitzmann, M. Schunter, and M. Waidner. How to break another "provably secure" payment system. *Lecture Notes in Computer Science*, 921:121–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Press:1989:CRC

[PT89] William H. Press and Saul A. Teukolsky. Cyclic redundancy checks for data integrity or identity. *Computers in Physics*, 3(4):88–??, July 1989. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). URL `https://aip.scitation.org/doi/10.1063/1.4822859`.

Phoenix:1995:QCP

[PT95] S. J. D. Phoenix and P. D. Townsend. Quantum cryptography: Protecting our future networks with quantum mechanics. *Lecture Notes in Computer Science*, 1025:112–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Parkes:1999:ACC

[PUF99] D. C. Parkes, L. H. Ungar, and D. P. Foster. Accounting for cognitive costs in online auction design. *Lecture Notes in Computer Science*, 1571:25–40, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Purdy:1974:HSL

[Pur74] George B. Purdy. A high security log-in procedure. *Communications of the Association for Computing Machinery*, 17(8):442–445, August 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `https://dl.acm.org/doi/10.1145/361082.361089`.

Puteanus:1627:EPC

[Put27] Erycius Puteanus. *EryclI Puteani Cryptographia Tassiana, sive, Clandestina scripti*. Typis Cornelii Coenesteynii, Louvanii, 1627. 18 + 2 pp. LCCN Z103.5 .P88 1627.

Preparata:1990:PCD

[PV90] F. P. Preparata and J. E. Vuillemin. Practical cellular dividers. *IEEE Transactions on Computers*, 39(5):

605–614, May 1990. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Peinado:1997:HPC

[PV97] M. Peinado and R. Venkatesan. Highly parallel cryptographic attacks. *Lecture Notes in Computer Science*, 1332:367–374, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Posegga:1998:BCV

[PV98] J. Posegga and H. Vogt. Byte code verification for Java smart cards based on model checking. *Lecture Notes in Computer Science*, 1485:175–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pluimakers:1986:ACS

[PvL86] G. M. J. Pluimakers and J. van Leeuwen. Authentication: a concise survey. *Computers and Security*, 5(3):243–250, September 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404886900155.

Preneel:1995:MMB

[PvO95] B. Preneel and P. C. van Oorschot. MD-x MAC and building fast MACs from hash functions. In Coppersmith [Cop95d], pages 1–14. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=963. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Preneel:1996:STM

[PvO96] B. Preneel and P. van Oorschot. On the security of two MAC algorithms. In Maurer [Mau96b], page ?? CODEN LNCSD9. ISBN 3-540-61186-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1996. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1070.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1070. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Pfitzmann:1986:NUO

[PW86a] A. Pfitzmann and M. Waidner. Networks without user observability — design options. In Pichler [Pic86], page ???? CODEN LNCSD9. ISBN 0-387-16468-5 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E961 1985. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1020.html`. "The workshop was sponsored by International Association for Cryptologic Research ... [et al.]"–T.p. verso.

Power:1986:AHE

[PW86b] June M. Power and Steve R. Wilbur. Authentication in a heterogeneous environment. *Computers and Security*, 5 (2):167, June 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404886901458`.

Pfitzmann:1987:NUO

[PW87a] Andreas Pfitzmann and Michael Waidner. Networks without user observability. *Computers and Security*, 6(2):158–166, April 1987. CODEN CPSEDU. ISSN 0167-4048. URL `http://www.semper.org/sirene/publ/PfWa_86anonyNetze.html`.

Power:1987:AHE

[PW87b] June M. Power and Steve R. Wilbur. Authentication in a heterogeneous environment. *Computers and Security*, 6(1):41–48, February 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887901246`.

Pfitzmann:1993:APS

[PW93a] Birgit Pfitzmann and Michael Waidner. Attacks on protocols for server-aided RSA computation. *Lecture Notes in Computer Science*, 658:153–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580153.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0658/06580153.pdf`.

Piper:1993:DSH

[PW93b] F. Piper and P. Wild. Digital signatures and hash functions. In Anonymous [Ano93d], pages 124–130. ISBN 1-85617-211-2. LCCN ????

Pfitzmann:1997:AF

[PW97a] B. Pfitzmann and M. Waidner. Anonymous fingerprinting. In Fumy [Fum97], pages 88–102. CODEN LNCSD9. ISBN 3-540-62975-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1997. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/062147.html`. Sponsored by the International Association for Cryptologic Research (IACR).

Pfitzmann:1997:AFL

[PW97b] B. Pfitzmann and M. Waidner. Asymmetric fingerprinting for larger collusion. In ACM [ACM97a], pages 151–160. ISBN 0-89791-912-2. LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/062148.html`.

Pfitzmann:1997:SLT

[PW97c] Birgit Pfitzmann and Michael Waidner. Strong loss tolerance of electronic coin systems. *ACM Transactions on Computer Systems*, 15 (2):194–213, May 1997. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tocs/1997-15-2/p194-pfitzmann/`.

Piper:1998:CSV

[PW98] Fred Piper and Michael Walker. Cryptographic solutions for voice telephony and GSM. *Network Security*, 1998(12):14–19, December 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485800876102`.

Piccardi:1999:CLD

[PW99] C. Piccardi and F. Wotawa. A communication language and the design of a diagnosis agent — towards a framework for mobile diagnosis agents. *Lecture Notes in Computer Science*, 1611: 420–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Polani:1999:DAR

[PWU99] D. Polani, S. Weber, and T. Uthmann. A direct approach to robot soccer agents: Description for the team MAINZ ROLLING BRAINS simulation league of RoboCup'98. *Lecture Notes in Computer Science*, 1604:390–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Podilchuk:1998:IAW

[PZ98] Christine I. Podilchuk and Wenjun Zeng. Image-adaptive watermarking using visual models. *IEEE Journal on Selected Areas in Communications*, 16(4): 525–539, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072141.html`.

Quisquater:1998:CSE

[Q+98] J.-J. (Jean-Jacques) Quisquater et al., editors. *Computer security, ESORICS 98: 5th European Symposium on Research in Computer Security, Louvain-la-Neuve, Belgium, September 16-18, 1998: proceedings*, volume 1485. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-65004-0. LCCN QA267.A1 L43 no.1485.

Quisquater:1991:CLE

[QD91] Jean-Jacques Quisquater and Yvo G. Desmedt. Chinese Lotto as an exhaustive code-breaking machine. *Computer*, 24(11):14–22, November 1991. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Quisquater:1989:BHF

[QG89] J. J. Quisquater and M. Girault. $2n$-bit hash-functions using n-bit symmetric block cipher algorithms. In Quisquater and Vandewalle [QV89], page ?? ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). LCCN QA76.9.A25 E964 1989. DM98.00.

Quisquater:1990:BHF

[QG90] J. J. Quisquater and M. Girault. $2n$-bit hash-functions using n-bit symmetric block cipher algorithms. In Quisquater and Vandewalle [QV90], pages 102–?? CODEN LNCSD9. ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1989; QA267.A1 L43 no.434. DM98.00. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340102.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0434/04340102.pdf`.

Quisquater:1995:ACE

[QG95] J.-J. Quisquater and Louis C. Guillou, editors. *Advances in cryptology, EUROCRYPT '95: International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21–25, 1995: proceedings*, volume 921 of *Lecture Notes in Computer*

Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-59409-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C794 1995.

Qiao:1998:CME

[QN98a] Lintian Qiao and Klara Nahrstedt. Comparison of MPEG encryption algorithms. *Computers and Graphics*, 22(4):437–448, August 1, 1998. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL `http://www.elsevier.com/cas/tree/store/cag/sub/1998/22/4/567.pdf`.

Qiao:1998:WMM

[QN98b] Lintian Qiao and Klara Nahrstedt. Watermarking methods for MPEG encoded video: Towards resolving rightful ownership. In IEEE [IEE98e], pages 276–285. ISBN 0-8186-8557-3, 0-8186-8559-X (microfiche). LCCN QA76.575.I623 1998. IEEE catalog number 98TB100241. IEEE Computer Society Order Number PR08557.

Qin:1988:RSS

[QSA88] Bin Qin, Howard A. Sholl, and Reda A. Ammar. RTS: a system to simulate the real time cost behaviour of parallel computations. *Software—Practice and Experience*, 18(10):967–985, October 1988. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Quisquater:1989:ACE

[QV89] Jean-Jacques Quisquater and Joos Vandewalle, editors. *Advances in Cryptology—EUROCRYPT '89: Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Belgium, April 10–13, 1989: Proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989. ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). LCCN QA76.9.A25 E964 1989. DM98.00.

Quisquater:1990:ACE

[QV90] Jean-Jacques Quisquater and Joos Vandewalle, editors. *Advances in cryptology — EUROCRYPT '89: Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Belgium, April 10–13, 1989: proceedings*, volume 434 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. CODEN LNCSD9. ISBN 0-387-53433-4 (New York), 3-

540-53433-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1989; QA267.A1 L43 no.434. DM98.00.

Quisquater:1998:E

[QV98] J.-J. Quisquater and J. Vandewalle. Eurocrypt '89. *Lecture Notes in Computer Science*, 1440:93–100, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rabin:1977:DS

[Rab77] M. O. Rabin. Digitalized signatures. In Richard A. DeMillo et al., editors, *Foundations of Secure Computation: Papers presented at a 3 day workshop held at Georgia Institute of Technology, Atlanta, October 1977*, pages x + 404. Academic Press, New York, NY, USA, 1977. ISBN 0-12-210350-5. LCCN QA76.9.A25 F66.

Rabin:1981:HES

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, Cambridge, MA, USA, 1981. URL `http://eprint.iacr.org/2005/187.pdf`.

Rabin:1989:EDI

[Rab89] Michael O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the Association for Computing Machinery*, 36(2):335–348, April 1989. CODEN JACOAH. ISSN 0004-5411. URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/62050.html`.

Rabin:1994:RSS

[Rab94] Tal Rabin. Robust sharing of secrets when the dealer is honest or cheating. *Journal of the Association for Computing Machinery*, 41(6):1089–1109, November 1994. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/195621.html`.

Rabin:1998:SAT

[Rab98] Tal Rabin. A simplified approach to threshold and proactive RSA. *Lecture Notes in Computer Science*, 1462:89–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620089.htm`; `http://link.springer-ny.com/link/service/series/`

0558/papers/1462/14620089.pdf.

Rackoff:1990:BTP

[Rac90] Charles Rackoff. A basic theory of public and private cryptosystems. *Lecture Notes in Computer Science*, 403:249–255, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Radlo:1997:LIC

[Rad97] E. J. Radlo. Legal issues in cryptography. *Lecture Notes in Computer Science*, 1318:259–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ramagopal:1992:DRB

[Ram92] S. Ramagopal. The *dictyostelium* ribosome: biochemistry, molecular biology, and developmental regulation. *Biochemistry and cell biology = Biochimie et biologie cellulaire*, 70(9): 738–750, September 1992. ISSN 0829-8211.

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].

Randell:1982:CGC

[Ran82a] Brian Randell. Colossus: Godfather of the computer (1977). In *The Origins of Digital Computers: Selected Papers* [Ran82b], pages 349–354. ISBN 0-387-11319-3, 3-540-11319-3. LCCN TK7885.A5 O741 1982.

Randell:1982:ODC

[Ran82b] Brian Randell, editor. *The Origins of Digital Computers: Selected Papers*. Texts and monographs in computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., third edition, 1982. ISBN 0-387-11319-3, 3-540-11319-3. xvi + 580 pp. LCCN TK7885.A5 O741 1982.

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].

Rao:1984:JEE

[Rao84] T. R. N. Rao. Joint encryption and error correction schemes. *ACM SIGARCH Computer Architecture News*, 12(3):240–241, June 1984. CODEN

CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Ratcliff:1996:DIN

[Rat96] Rebecca Ann Ratcliff. *Delusions of intelligence: national cultures of cryptology, secrecy and bureaucracy in Germany and Britain during World War II*. Thesis (Ph.D. in rhetoric), Department of Rhetoric, University of California, Berkeley, Berkeley, CA, USA, December 1996. xix + 303 pp.

Rhodes-Burke:1982:RSA

[RB82] Robert Rhodes-Burke. Retrofitting for signature analysis simplified. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 33(1):9–16, January 1982. CODEN HPJOAX. ISSN 0018-1153.

Reiter:1994:HSR

[RB94] Michael K. Reiter and Kenneth P. Birman. How to securely replicate services. *ACM Transactions on Programming Languages and Systems*, 16(3):986–1009, May 1994. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0164-0925/177745.html.

Ramesh:1999:VPP

[RB99] S. Ramesh and P. Bhaduri. Validation of pipelined processor designs using Esterel tools. *Lecture Notes in Computer Science*, 1633: 84–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rowstron:1999:CUR

[RBCE99] A. Rowstron, B. Bradshaw, D. Crosby, and T. Edmonds. The Cambridge University Robot Football Team description. *Lecture Notes in Computer Science*, 1604:422–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rabin:1989:VSS

[RBO89] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In ACM [ACM89a], pages 73–85. ISBN 0-89791-326-4. LCCN QA 76.9 D5 A26 1989.

Reiter:1994:SAF

[RBvR94] Michael K. Reiter, Kenneth P. Birman, and Robbert van Renesse. A security architecture for fault-tolerant systems. *ACM Transactions on Computer Systems*, 12(4):340–371, November 1994. CODEN

ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic). URL http://www.acm.org:80/pubs/citations/journals/tocs/1994-12-4/p340-reiter/.

Rogaway:1994:SEA

[RC94a] P. Rogaway and D. Coppersmith. A software-optimised encryption algorithm. *Lecture Notes in Computer Science*, 809: 56–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rogaway:1994:SOE

[RC94b] P. Rogaway and D. Coppersmith. A software-optimised encryption algorithm. *Lecture Notes in Computer Science*, 809: 56–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Russinovich:1995:EWL

[RC95] Mark Russinovich and Bryce Cogswell. Examining the Windows 95 Layered File System. *Dr. Dobb's Journal of Software Tools*, 20(12):60, 62, 66, 68–70, 108–110, December 1995. CODEN DDJOEB. ISSN 1044-789X.

Rubia:1999:RIB

[RCM99] Montse Rubia, Juan Carlos Cruellas, and Manel Medina. Removing interoperability barriers between the X.509 and EDIFACT public key infrastructures: The DEDICA Project. *Lecture Notes in Computer Science*, 1560:245–262, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1560/15600245.htm; http://link.springer-ny.com/link/service/series/0558/papers/1560/15600245.pdf.

Renvall:1996:ASS

[RD96a] A. Renvall and C. Ding. The access structure of some secret-sharing schemes. *Lecture Notes in Computer Science*, 1172:67–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Renvall:1996:NSS

[RD96b] A. Renvall and C. Ding. A nonlinear secret sharing scheme. *Lecture Notes in Computer Science*, 1172: 56–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Roback:1999:CRF

[RD99a] Edward Roback and Morris Dworkin. Conference report: First Advanced Encryption Standard (AES)

Candidate Conference, Ventura, CA, August 20–22, 1998. *Journal of research of the National Institute of Standards and Technology*, 104(1):97–105, January/February 1999. CODEN JRITEF. ISSN 1044-677X (print), 2165-7254 (electronic). URL http://csrc.nist.gov/encryption/aes/round1/conf1/j41ce-rob.pdf.

Roback:1999:FAE

[RD99b] Edward Roback and Morris Dworkin. First Advanced Encryption Standard (AES) candidate conference. *CryptoBytes*, 4(2): 6–14, Winter 1999. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n2.pdf.

Rebel:1998:ADS

[RDK98] Thomas F. Rebel, Olaf Darge, and Wolfgang Koenig. Approaches of digital signature legislation. *Lecture Notes in Computer Science*, 1402:39–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1402/14020039.htm; http://link.springer-ny.com/link/service/series/0558/papers/1402/14020039.pdf.

Rijmen:1996:CS

[RDPB96] V. Rijmen, J. Daemen, B. Preneel, and A. Bosselaers. The cipher shark. *Lecture Notes in Computer Science*, 1039:99–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Reeds:1979:CMC

[Ree79] James Reeds. Cracking a multiplicative congruential encryption algorithm. In *Information linkage between applied mathematics and industry (Proc. First Annual Workshop, Naval Postgraduate School, Monterey, Calif., 1978)*, pages 467–472. Academic Press, New York, NY, USA, 1979.

Rees:1997:AGO

[Ree97] Frank Rees. Australian Government obstructs the export of revolutionary encryption. *Network Security*, 1997(11):7–8, November 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897900775.

Reeds:1998:SCB

[Ree98] J. Reeds. Solved: The ciphers in Book III of Trithemius's Steganographia. *Cryptologia*, 22(4):291–317, October 1998. CODEN CRYPE6. ISSN

0161-1194 (print), 1558-1586 (electronic). URL http://www.avesta.org/tritheim/stegano.htm; http://www.nsa.gov:8080/museum/tour.html; http://www.research.att.com/~reeds/trit.ps. See [Tri06a, Tri06b, Tri06c, Sch20, Tri21a, Tri21b, Tri21c, Sch33, Hei76, Wal00, Shu82].

Reischuk:1985:NSB

[Rei85] R. Reischuk. A new solution to the Byzantine generals problem. *Information and Control*, pages 23–42, 1985. CODEN IFCNA4. ISSN 0019-9958 (print), 1878-2981 (electronic).

Reiter:1992:ISG

[Rei92] Michael Reiter. Integrating security in a group oriented distributed system. *Operating Systems Review*, 26(2): 27, April 1992. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Reiter:1996:DTR

[Rei96] Michael K. Reiter. Distributing trust with the Rampart Toolkit. *Communications of the Association for Computing Machinery*, 39(4):71–74, April 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/227228.html; http://www.acm.org/pubs/toc/Abstracts/cacm/227228.html.

Rejewski:1977:ATP

[Rej77] Marian Rejewski. An application of the theory of permutations in breaking the Enigma cipher. *Applications of Mathematicae, Polish Academy of Sciences*, 16 (??):543–559, ???? 1977.

Rejewski:1981:HPM

[Rej81] Marian Rejewski. How Polish mathematicians deciphered the Enigma. *Annals of the History of Computing*, 3(3):213–234, July/September 1981. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1981/pdf/a3213.pdf; http://www.computer.org/annals/an1981/a3213abs.htm. Afterwords by Cipher A. Deavours and I. J. Good. This article was entitled “Jak matematycy polscy rozszyfrowz Enigmgę” in the Annals of the Polish Mathematical Society, Series II, Wiadomości Matematyczne, Volume 23, 1980, 1-28, translated by Joan Stepenske. See minor correction [Ano81a].

Rejewski:19xx:EMH

[Rejxx] Marian Rejewski. Enigma

(1930–40). method and history of solving the German machine cipher. Unpublished manuscript in Polish, 19xx.

Revello:1991:CEC

[Rev91] Timothy E. Revello. A combination of exponentiation ciphers and the data encryption standard as a pseudorandom number generator. Thesis (M.S.), Rensselaer Polytechnic Institute at The Hartford Graduate Center, Troy, NY, USA, 1991. viii + 68 pp.

Reynard:1996:SCB

[Rey96] Robert Reynard. *Secret code breaker: a cryptanalyst's handbook*. Smith and Daniel Marketing, Jacksonville, FL, USA, 1996. ISBN 1-889668-00-1. 92 pp. LCCN Z103 .R49 1996.

Reynard:1997:SCB

[Rey97] Robert Reynard. *Secret code breaker II a cryptanalyst's handbook*. Smith and Daniel Marketing, Jacksonville, FL, USA, 1997. ISBN 1-889668-06-0. viii + 120 pp. LCCN ????

Reynard:1999:SCB

[Rey99] Robert Reynard. *Secret code breaker III: a cryptanalyst's handbook*. Smith and Daniel Marketing, Jacksonville Beach, FL, USA, 1999. ISBN 1-889668-13-3. 117 pp. LCCN Z103 .R493 1999.

Rowlett:1935:FAP

[RF35] Frank B. Rowlett and William F. Friedman. *Further applications of the principles of indirect symmetry of position in secondary alphabets: technical paper*. United States Government Printing Office, Washington, DC, USA, 1935. ???? pp.

Reiter:1996:KMS

[RFLW96] Michael K. Reiter, Matthew K. Franklin, John B. Lacy, and Rebecca N. Wright. The Ω key management service. *Journal of Computer Security*, 4(4):267–287, ???? 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Reiter:1995:SCR

[RG95] Michael Reiter and Li Gong. Securing causal relationships in distributed systems. *The Computer Journal*, 38(8):633–642, ???? 1995. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/Volume_38/Issue_08/Vol38_08.body.html#AbstractReiter`.

Rhodes:1999:SPH

[RG99] D. L. Rhodes and A. Gerasoulis. Scalable parallelization of harmonic balance simulation. *Lecture Notes in Computer Science*, 1586: 1055–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Radu:1997:WHR

[RGV97] C. Radu, R. Govaerts, and J. Vandewalle. Witness hiding restrictive blind signature scheme. *Lecture Notes in Computer Science*, 1355: 283–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rubin:1993:LRJ

[RH93] A. D. Rubin and P. Honeyman. Long running jobs in an authenticated environment. In USENIX Association [USE93], pages 19–28. ISBN 1-880446-55-3. LCCN QA 76.9 A25 U54 1993. URL `http://www.usenix.org/publications/library/proceedings/sec4/`.

Ryu:1999:PAA

[RH99] M. Ryu and S. Hong. A period assignment algorithm for real-time system design. *Lecture Notes in Computer Science*, 1579:34–43, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rivest:1992:RNP

[RHAL92] Ronald L. Rivest, Martin E. Hellman, John C. Anderson, and John W. Lyons. Responses to NIST's proposal. *Communications of the Association for Computing Machinery*, 35(7): 41–54, July 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/129905.html`.

Rhee:1993:RAC

[Rhe93] Man Y. Rhee. Research activities on cryptology in Korea. *Lecture Notes in Computer Science*, 739:179–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rhee:1994:CSC

[Rhe94] Man Young Rhee. *Cryptography and secure communications*. McGraw-Hill series on computer communications. McGraw-Hill, New York, NY, USA, 1994. ISBN 0-07-112502-7. xxiii + 504 pp. LCCN QA76.9.A25R5 1994.

Rhoads:1995:SMA

[Rho95] Geoffrey B. Rhoads. *Steganography: methods and applications*. Pinecone Press, 363 S.W. Tualatin Loop, West Linn, OR 97068, USA, 1995. 98 pp.

Richards:1974:SWP

[Ric74] Sheila R. Richards. *Secret writing in the public records: Henry VIII–George II*. London, 1974. x + 173 + 4 plates pp. UK£4.50. Contains one hundred documents, all but one of which are written wholly or partially in cipher and are now deciphered and printed in full for the first time. Includes letters in French or Italian, with a summary in English.

Rihaczek:1987:T

[Rih87] Karl Rihaczek. Teletrust. *Computer Networks and ISDN Systems*, 13(3):235–239, 1987. CODEN CNISE9. ISSN 0169-7552.

Rijmen:1999:WL

[Rij99] Vincent Rijmen. Weaknesses in LOKI97. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm`; `http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf`; `http://www.nist.gov/aes`. No slides for the conference talk are available.

Riley:1996:LET

[Ril96] W. D. Riley. LANSCAPE — encrypt this!! — there are a thousand reasons to use encryption. unfortunately, the current state of technology does not lend itself to e-mail platforms. *Datamation*, 42(9):27–??, ???? 1996. CODEN DTMNAT. ISSN 0011-6963.

Ripe:1995:IPS

[RIP95a] RIPE. Integrity primitives for secure information systems. final report of RACE integrity primitives evaluation (RIPE-RACE 1040). In Bosselaers and Preneel [BP95b], page ?? CODEN LNCSD9. ISBN 3-540-60640-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I553 1995.

RIPE:1995:RIP

[RIP95b] RIPE Consortium. Ripe integrity primitives — final report of RACE integrity primitives evaluation (R1040). In Bosselaers and Preneel [BP95b], page ?? CODEN LNCSD9. ISBN 3-540-60640-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I553 1995.

Ritter:1999:IWC

[Rit99] Terry Ritter. Internet watch: Cryptography: Is staying with the herd really best? *Computer*, 32(8): 94–95, August 1999. CODEN CPTRB4. ISSN 0018-

9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co1999/pdf/r8094.pdf.

Ritchie:19xx:DCW

[Ritxx] Dennis M. Ritchie. Dabbling in the cryptographic world — a story. This undated note describes the interesting history behind the non-publication of a paper [RRM78] on the Hagelin cypher machine (M-209), submitted to the journal Cryptologia, because of shadowy suggestions of a "retired gentleman from Virginia"., 19xx. URL http://www.cs.bell-labs.com/~dmr/crypt.html.

Rivest:1974:HCA

[Riv74a] R. L. Rivest. On hash-coding algorithms for partial-match retrieval. In IEEE [IEE74], pages 95–103.

Rivest:1974:AAR

[Riv74b] Ronald L. Rivest. Analysis of associative retrieval algorithms. Technical Report TR.54, Institut de la Recherche en Informatique et Automatique, now Institut National de Recherche en Informatique et Automatique (INRIA), Domaine de Voluceau — Rocquencourt — B.P. 105, 78153 Le Chesnay Cedex, France, February 1974. ?? pp. Also published in/as: Stanford CSD report 74-415. Also published in/as: SIAM Journal for Computing, Springer-Verlag (Heidelberg, FRG and New York NY, USA)-Verlag, 1976, with mod. title.

Rivest:1979:CRC

[Riv79] Ronald L. Rivest. Critical remarks on: "Critical remarks on some public-key cryptosystems" [BIT **18**(4), 1978, pp. 493–496; MR 80b:94033] by Tore Herlestam. *BIT*, 19(2): 274–275, June 1979. CODEN NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=19&issue=2&spage=274. See [Her78].

Rivest:1980:DSC

[Riv80] R. L. Rivest. A description of a single-chip implementation of the RSA cipher. *Lambda: the magazine of VLSI design*, 1 (3):14–18, Fourth Quarter 1980. CODEN VDESDP. ISSN 0273-8414.

Rivest:1985:RCP

[Riv85] Ronald L. Rivest. RSA chips (past/present/future). In Beth et al. [BCI85], pages 159–163. CODEN

LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0209.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=209. Held at the University of Paris, Sorbonne.

Rivest:1987:EDR

[Riv87] Ronald L. Rivest. The eary days of RSA: History and lessons. In Ashenhurst [Ash87], page ?? ISBN 0-201-07794-9. LCCN QA76.24 .A33 1987. ACM Turing Award lecture.

Rivest:1990:RMM

[Riv90a] R. L. Rivest. RFC 1186: MD4 message digest algorithm, October 1, 1990. URL ftp://ftp.internic.net/rfc/rfc1186.txt; https://www.math.utah.edu/pub/rfc/rfc1186.txt. Status: INFORMATIONAL.

Rivest:1990:C

[Riv90b] Ron Rivest. Cryptography. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science*, pages 717–755. Elsevier, Amsterdam, The Netherlands, 1990. ISBN 0-444-88075-5 (Elsevier: set), 0-444-88071-2 (Elsevier: vol. A), 0-444-88074-7 (Elsevier: vol. B), 0-262-22040-7 (MIT Press: set), 0-262-22038-5 (MIT Press: vol. A), 0-262-22039-3 (MIT Press: vol. B). LCCN QA76 .H279 1990.

Rivest:1991:FFM

[Riv91a] R. L. Rivest. Finding four million large random primes. *Lecture Notes in Computer Science*, 537: 625–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rivest:1991:MMD

[Riv91b] R. L. Rivest. The MD4 message digest algorithm. In Menezes and Vanstone [MV91], pages 303–311. CODEN LNCSD9. ISBN 0-387-54508-5 (New York), 3-540-54508-5 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1990. Conference held Aug. 11–15, 1990, at the University of California, Santa Barbara.

Rivest:1992:RMMa

[Riv92a] R. Rivest. RFC 1320: The MD4 message-digest algorithm, April 1992. URL ftp://ftp.internic.net/rfc/rfc1320.txt; https://www.math.utah.edu/pub/rfc/rfc1320.txt. Status: INFORMATIONAL.

Rivest:1992:RMMb

[Riv92b] R. Rivest. RFC 1321: The MD5 message-digest algorithm, April 1992. URL `ftp://ftp.internic.net/rfc/rfc1321.txt`; `https://www.math.utah.edu/pub/rfc/rfc1321.txt`. Status: INFORMATIONAL.

Rivest:1993:DRR

[Riv93a] R. Rivest. Dr. Ron Rivest on the difficulty of factoring ciphertext. *The RSA Newsletter*, 1(1):??, Fall 1993. reprinted, in an updated form, in an appendix on pages 361-364 in S. Garfinkel, PGP: Pretty Good Privacy, O'Reilly & Associates, 1995.

Rivest:1993:CML

[Riv93b] Ronald L. Rivest. Cryptography and machine learning. *Lecture Notes in Computer Science*, 739:427–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rivest:1993:NPD

[Riv93c] Ronald L. Rivest. On NIST's proposed Digital Signature Standard. *Lecture Notes in Computer Science*, 739:481–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rivest:1995:DRR

[Riv95a] R. L. Rivest. Dr. Ron Rivest on the difficulty of factoring. First published in Ciphertext: The RSA Newsletter, vol. 1, no. 1, fall 1993, and reprinted, in an updated form, in an appendix on pp. 361–364 in S. Garfinkel, PGP: Pretty Good Privacy, O'Reilly & Associates [**?**]., 1995.

Rivest:1995:REAb

[Riv95b] R. L. Rivest. The RC5 encryption algorithm. In Preneel [Pre95a], pages 86–96. CODEN LNCSD9. ISBN 3-540-60590-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F37 1995.

Rivest:1995:REAa

[Riv95c] Ronald L. Rivest. The RC5 encryption algorithm. *Dr. Dobb's Journal of Software Tools*, 20(1):146, 148, January 1995. CODEN DDJOEB. ISSN 1044-789X.

Rivest:1995:REAc

[Riv95d] Ronald L. Rivest. The RC5 encryption algorithm. *CryptoBytes*, 1(1):9–11, Spring 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n1.pdf`.

Rivest:1995:WC

[Riv95e] Ronald L. Rivest. Welcome to CryptoBytes. *Crypto-*

Bytes, 1(1):2, Spring 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n1.pdf.

Rivest:1997:ELT

[Riv97a] R. L. Rivest. Electronic lottery tickets as micropayments. *Lecture Notes in Computer Science*, 1318: 307–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rivest:1997:PFC

[Riv97b] R. L. Rivest. Perspectives on financial cryptography. *Lecture Notes in Computer Science*, 1318:145–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rivest:1997:ANE

[Riv97c] Ronald L. Rivest. All-or-nothing encryption and the package transform. In Biham [Bih97c], pages 210–?? CODEN LNCSD9. ISBN 3-540-63247-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25F77 1997. URL http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670210.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670210.pdf; http://theory.lcs.mit.edu/~rivest/fusion.ps.

Rivest:1998:RDR

[Riv98a] R. Rivest. RFC 2268: a description of the RC2(r) encryption algorithm, January 1998. URL ftp://ftp.internic.net/rfc/rfc2268.txt; https://www.math.utah.edu/pub/rfc/rfc2268.txt. Status: INFORMATIONAL.

Rivest:1998:CWE

[Riv98b] R. L. Rivest. Can we eliminate certificate revocations lists? *Lecture Notes in Computer Science*, 1465: 178–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rivest:1998:CAR

[Riv98c] Ronald L. Rivest. The case against regulating encryption technology: One of the pioneers of computer security says the U.S. government should keep its hands off cryptography. *Scientific American*, 279(4): 116–117 (Intl. ed. 88–??), October 1998. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/1998/1098issue/1098currentissue.html.

Rivest:1998:CWC

[Riv98d] Ronald L. Rivest. Chaffing and winnowing: Confidentiality without encryption. *CryptoBytes*, 4(1):12–17, Summer 1998. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto4n1.pdf.

Rivest:19xx:PC

[Rivxx] R. Rivest. Personal communication. ????, 19xx.

Rhodes:1993:ZF

[RK93] Daniela Rhodes and Aaron Klug. Zinc fingers. *Scientific American*, 268(2):56–?? (Intl. ed. 32–??), February 1993. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Rijmen:1998:WL

[RK98a] V. Rijmen and L. R. Knudsen. Weaknesses in LOKI97. Technical report, Katholieke Universiteit Leuven, Leuven, Belgium, June 15, 1998. URL ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/rijmen/loki97.ps.gz.

Rowlett:1998:SMM

[RK98b] Frank B. (Frank Byron) Rowlett and David Kahn. *The story of MAGIC: memoirs of an American cryptologic pioneer*. Aegean Park Press, Laguna Hills, CA, USA, 1998. ISBN 0-89412-273-8. x + 258 + 8 pp. LCCN D810.C88 R68 1998.

Roy:1999:QCE

[RK99] S. Roy and G. Kar. Quantum cryptography, eavesdropping, and unsharp spin measurement. *Lecture Notes in Computer Science*, 1509:214–217, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rosenson:1994:GWE

[RKD94] Beth Rosenson, Stephen Thomas Kent, and Dorothy Elizabeth Robling Denning. Government wiretapping, encryption and the Clipper chip debate. Seminar notes, MIT Communications Forum, Cambridge, MA, USA, September 29, 1994. 4 + 6 pp.

Ruanaidh:1996:WDI

[RKDB96] Ó Ruanaidh, J. J. K., W. J. Dowling, and F. M. Boland. Watermarking digital images for copyright protection. *IEE proceedings. Vision, image, and signal processing*, 143(4):250–256, August 1996. CODEN IVIPEK. ISSN 1350-245X. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1031.html.

Reeds:1985:NPR

[RM85] J. A. Reeds and J. L. Manferdelli. DES has no per round linear factors. In Blakley and

Chaum [BC85], pages 377–389. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=377. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Rao:1987:PKA

[RN87] T. R. N. Rao and Kil-Hyun Nam. Private-key algebraic-coded cryptosystems. *Lecture Notes in Computer Science*, 263:35–48, 1987. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rao:1989:PKA

[RN89] T. R. N. Rao and Kil-Hyun Nam. Private-key algebraic-code encryptions. *IEEE Transactions on Information Theory*, IT-35(4):829–833, 1989. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Raisch:1996:ACH

[RO96] J. Raisch and S. O'Young. A DES approach to control of hybrid dynamical systems. *Lecture Notes in Computer Science*, 1066:563–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Roberts:1993:ECI

[Rob93] D. W. Roberts. Evaluation criteria for IT security. *Lecture Notes in Computer Science*, 741:151–161, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Robshaw:1995:BC

[Rob95a] M. J. B. Robshaw. Block ciphers. Technical Report TR-601, RSA Data Security, Inc., Redwood City, CA, USA, July 1995. Version 2.0.

Robshaw:1995:SC

[Rob95b] M. J. B. Robshaw. Stream ciphers. Technical Report TR-701, RSA Data Security, Inc., Redwood City, CA, USA, July 25, 1995. 46 pp. URL ftp://ftp.rsasecurity.com/pub/pdfs/tr701.pdf.

Roberts:1998:SMP

[Rob98a] D. W. Roberts. Security management — the process. *Lecture Notes in*

Computer Science, 1528: 366–376, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Robinson:1998:FRC

[Rob98b] Bill Robinson. The fall and rise of cryptanalysis in Canada. In Deavours et al. [DKK+98], pages 77–92. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Roe:1994:PSC

[Roe94] M. Roe. Performance of symmetric ciphers and one-way hash functions. *Lecture Notes in Computer Science*, 809:83–89, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Roe:1995:PBC

[Roe95] M. Roe. Performance of block ciphers and hash functions — one year later. *Lecture Notes in Computer Science*, 1008:359–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Roelse:1999:CWD

[Roe99] Peter Roelse. Cryptanalysis of the Wu-Dawson public key cryptosystem. *Finite Fields and their Applications*, 5(4):386–392, 1999. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic).

Rogaway:1995:BHA

[Rog95] Phillip Rogaway. Bucket hashing and its application to fast message authentication. *Lecture Notes in Computer Science*, 963: 29–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630029.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0963/09630029.pdf`.

Rogaway:1996:SD

[Rog96] Phillip Rogaway. The security of DESX. *CryptoBytes*, 2(2):8–11, Summer 1996. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto2n2.pdf`.

Rohwer:1975:GIM

[Roh75] Jurgen Rohwer. *Geleitzugschlachten im Marz 1943: Führungsprobleme im Höhepunkt der Schlacht im Atlantik. (German) [Convoy in March 1943: implementation problems in the climax of the Battle of the Atlantic]*. Motorbuch, Stuttgart, Germany, 1975.

ISBN 3-87943-383-6. 356 pp. LCCN ???? See also English translation [Roh77].

Rohwer:1977:CCB

[Roh77] Jürgen Rohwer. *The critical convoy battles of March 1943: the battle for HX.229/SC122*. Naval Institute Press, Annapolis, MD, USA, 1977. ISBN 0-87021-818-2. 256 + 32 pp. LCCN D770 .R59313. Revised English translation by Derek Masters of the German original [Roh75].

Rohatgi:1999:CNR

[Roh99] Pankaj Rohatgi. A cautionary note regarding evaluation of AES candidates on smart-cards. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? No slides for the conference talk are available.

Roman:1990:C

[Rom90a] Steven Roman. *Cryptology*. Modules in mathematics. Innovative textbooks, Irvine, CA, USA, second edition, 1990. ISBN 1-878015-06-0. various pp. LCCN ????

Rompel:1990:OWF

[Rom90b] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In ACM [ACM90], pages 387–394. ISBN 0-89791-361-2. LCCN QA76.A15 1990. URL `http://www.acm.org/pubs/citations/proceedings/stoc/100216/p387-rompel/`. ACM order no. 508900.

Rose:1993:RCM

[Ros93] M. Rose. RFC 1544: The content-MD5 header field, November 1993. URL `ftp://ftp.internic.net/rfc/rfc1544.txt`; `ftp://ftp.internic.net/rfc/rfc1864.txt`; `https://www.math.utah.edu/pub/rfc/rfc1544.txt`; `https://www.math.utah.edu/pub/rfc/rfc1864.txt`. Obsoleted by RFC1864 [MR95b]. Status: PROPOSED STANDARD.

Rosen:1994:EMT

[Ros94] Helen Rosen. Encryption and metering technology: new data security and pricing options for CD-ROM (and other digital media). Business information services 0434, LINK Resources Corp., 79 Fifth Ave., New York, NY 10003, USA, January 1994. 9 pp.

Rose:1995:PPZ

[Ros95a] Greg Rose. PGP, Phil Zimmerman, Life, the universe, and so on. *;login: the USENIX Association newsletter*, 20(2):4–7, April 1995. CODEN

LOGNEM. ISSN 1044-6397.

Rose:1995:SUP

[Ros95b] Greg Rose. Status update on PGP and legal actions. *;login: the USENIX Association newsletter*, 20(5):9–??, October 1995. CODEN LOGNEM. ISSN 1044-6397.

Rose:1996:IUP

[Ros96a] Greg Rose. Instructions for the USENIX PGP key-signing. *;login: the USENIX Association newsletter*, 21 (4):10–??, August 1996. CODEN LOGNEM. ISSN 1044-6397.

Rose:1996:PMI

[Ros96b] Greg Rose. The PGP moose — implementation and experience. In USENIX [USE96a], pages 155–160. URL http://www.usenix.org/publications/library/proceedings/lisa96/ggr.html.

Rose:1996:PZH

[Ros96c] Greg Rose. Phil Zimmermann is off the hook. *;login: the USENIX Association newsletter*, 21(2):6–??, April 1996. CODEN LOGNEM. ISSN 1044-6397.

Rose:1996:UCI

[Ros96d] Greg Rose. Update on cryptography issues. *;login: the USENIX Association newsletter*, 21(1):4–??, February 1996. CODEN LOGNEM. ISSN 1044-6397.

Rose:1996:UPKa

[Ros96e] Greg Rose. USENIX PGP key-signing service. *;login: the USENIX Association newsletter*, 21(3):10–??, June 1996. CODEN LOGNEM. ISSN 1044-6397.

Rose:1996:UPKb

[Ros96f] Greg Rose. USENIX PGP key-signing service. *;login: the USENIX Association newsletter*, 21(4):8–??, August 1996. CODEN LOGNEM. ISSN 1044-6397.

Rose:1997:PZP

[Ros97a] Bruce D. Rose. Phil Zimmermann's Pretty Good Privacy: issues, history, and mechanics. Thesis (B.S.), California Polytechnic State University, San Luis Obispo, CA, USA, 1997. ii + 22 pp.

Rose:1997:UUP

[Ros97b] Greg Rose. Update on the USENIX PGP key signing service. *;login: the USENIX Association newsletter*, 22 (1):6–??, February 1997. CODEN LOGNEM. ISSN 1044-6397.

Rosenheim:1997:CIS

[Ros97c] Shawn James Rosenheim. *The cryptographic imagina-*

tion: secret writing from Edgar Poe to the Internet. The Johns Hopkins University Press, Baltimore, MD, USA, 1997. ISBN 0-8018-5331-1 (hardcover), 0-8018-5332-X (paperback). ix + 264 pp. LCCN PS2642.C5 R67 1997.

Rose:1998:SCB

[Ros98a] G. Rose. A stream cipher based on linear feedback over GF(208). *Lecture Notes in Computer Science*, 1438:135–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rose:1998:NUP

[Ros98b] Greg Rose. News from the USENIX PGP key signing service. *;login: the USENIX Association newsletter*, 23(2):??, April 1998. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/1998-4/pgp.html.

Rose:1998:UPK

[Ros98c] Greg Rose. USENIX PGP key signing service to be discontinued. *;login: the USENIX Association newsletter*, 23(5):??, August 1998. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/1998-8/tcpip.html.

Rosenfeld:1999:GGW

[Ros99] Megan Rosenfeld. "Government girls": World War II's Army of the Potomac. *Washington Post*, ??(??):??, May 10, 1999.

Rarity:1994:QRN

[ROT94] J. G. Rarity, P. C. M. Owens, and P. R. Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics*, 41(12):2435–2444, ???? 1994. CODEN JMOPEW. ISSN 0950-0340 (print), 1362-3044 (electronic). URL http://www.tandfonline.com/doi/abs/10.1080/09500349414552281.

Rotenberg:1995:ECP

[Rot95a] Marc Rotenberg. *1995 EPIC cryptography and privacy sourcebook: documents on encryption policy, wiretapping and information warfare*. Electronic Privacy Information Center, Washington, DC, USA, 1995. various pp.

Rothenberg:1995:ELD

[Rot95b] Jeff Rothenberg. Ensuring the longevity of digital documents. *Scientific American*, 272(1):42–47 (Intl. ed. 24–??), January 1995. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Rothke:1997:WED

[Rot97] Ben Rothke. Want to encrypt data? Try Triple-DES. *Datamation*, 43(3): 122–??, ???? 1997. CODEN DTMNAT. ISSN 0011-6963.

Routh:1984:PAA

[Rou84] Richard LeRoy Routh. A proposal for an architectural approach which apparently solves all known software-based internal computer security problems. *Operating Systems Review*, 18(3):31–39, July 1984. CODEN OSRED8. ISSN 0163-5980.

Roy:1986:CBI

[Roy86] Marc Paul Roy. A CMOS bit-slice implementation of the RSA public key encryption algorithm. Thesis (M.Sc.(Eng.)), Queen's University, Ottawa, ON, Canada, 1986. 3 microfiches (210 fr.).

Redding:1994:LPF

[RP94] Christopher Redding and William J. Pomper. Linking protection in Federal Standard 1045 HF radios using the Data Encryption Standard. NTIA report 92-289, U.S. Department of Commerce, National Telecommunications and Information Administration, Washington, DC, USA, 1994. ?? pp.

Rijmen:1995:CM

[RP95a] V. Rijmen and B. Preneel. Cryptanalysis of McGuffin. *Lecture Notes in Computer Science*, 1008:353–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rijmen:1995:ICD

[RP95b] V. Rijmen and B. Preneel. Improved characteristics for differential cryptanalysis of hash functions based on block ciphers. *Lecture Notes in Computer Science*, 1008: 242–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rijmen:1997:FTC

[RP97a] Vincent Rijmen and Bart Preneel. A family of trapdoor ciphers. *Lecture Notes in Computer Science*, 1267: 139–148, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670139.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670139.pdf`.

Rogowitz:1997:HVE

[RP97b] Bernice E. Rogowitz and Thrasyvoulos N. Pappas, editors. *Human vision and* *electronic imaging II: 10–13 February 1997, San Jose, California*, volume 3016 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 1997. ISBN 0-8194-2427-7. LCCN TS510.S63 v.3016.

Risager:1998:SDO

[RP98] C. Risager and J. W. Perram. Ship design optimization. *Lecture Notes in Computer Science*, 1541: 476–482, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ringeisen:1986:ADM

[RR86] Richard D. Ringeisen and Fred S. Roberts, editors. *Applications of discrete mathematics. Proceedings of the Third SIAM Conference on Discrete Mathematics held at Clemson University, Clemson, South Carolina, May 14–16, 1986*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1986. ISBN 0-89871-219-X. LCCN QA76.9.M35C65 1986.

Reeds:1978:HCM

[RRM78] J. Reeds, D. Ritchie, and R. Morris. The Hagelin cypher machine (M-209): Cryptanalysis from ciphertext alone. Submitted to the journal Cryptologia, but never published. For the story behind the suppression of publication, see [Ritxx]. Internal technical memoranda TM 78-1271-10, TM 78-1273-2., 1978.

Rauber:1997:SDW

[RRP97] Ch. Rauber, J. O. Ruanaidh, and Th. Pun. Secure distribution of watermarked images for a digital library of ancient papers. In Allen and Rasmussen [AR97], pages 123–130. ISBN 0-89791-868-1. LCCN Z 699 A1 A27 1997. ACM order number 606971.

Rigney:1997:RRAa

[RRSW97a] C. Rigney, A. Rubens, W. Simpson, and S. Willens. RFC 2058: Remote authentication dial in user service (RADIUS), January 1997. URL `ftp://ftp.internic.net/rfc/rfc2058.txt`; `ftp://ftp.internic.net/rfc/rfc2138.txt`; `https://www.math.utah.edu/pub/rfc/rfc2058.txt`; `https://www.math.utah.edu/pub/rfc/rfc2138.txt`. Obsoleted by RFC2138 [RRSW97b]. Status: PROPOSED STANDARD.

Rigney:1997:RRAb

[RRSW97b] C. Rigney, A. Rubens, W. Simpson, and S. Willens. RFC 2138: Remote authentication dial in user service (RADIUS), April 1997. URL ftp://ftp.internic.net/rfc/rfc2058.txt; ftp://ftp.internic.net/rfc/rfc2138.txt; https://www.math.utah.edu/pub/rfc/rfc2058.txt; https://www.math.utah.edu/pub/rfc/rfc2138.txt. Obsoletes RFC2058 [RRSW97a]. Status: PROPOSED STANDARD.

Rivest:1998:RBC

[RRSY98] Ronald L. Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin. The RC6 block cipher: a simple fast secure AES proposal. In National Institute of Standards and Technology [Nat98], page 19. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf1/rc6-slides.pdf; http://people.csail.mit.edu/rivest/pubs/RRSY98.pdf. Only the slides for the conference talk are available.

Rivest:1983:RET

[RS83] Ronald L. Rivest and Alan T. Sherman. Randomized encryption techniques. Technical report MIT/LCS/TM-234, Massachusetts Institute of Technology, Laboratory for Computer Science, Cambridge, MA, USA, 1983. 20 pp.

Rivest:1984:HEE

[RS84] Ronald L. Rivest and Adi Shamir. How to expose an eavesdropper. *Communications of the Association for Computing Machinery*, 27(4):393–395, April 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Rackoff:1991:NIZ

[RS91] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. *Lecture Notes in Computer Science*, 576:433–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760433.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760433.pdf.

Rackoff:1993:CDA

[RS93] Charles Rackoff and Daniel R. Simon. Cryptographic defense against traffic analysis. In ACM [ACM93b], pages 672–681. ISBN 0-89791-591-7. LCCN QA 76.6 A13 1993. ACM order no. 508930.

Rescorla:1996:SHT

[RS96a] E. Rescorla and A. Schiffman. The secure HyperText transfer protocol. Internet draft draft-ietf-wts-shttp-01.txt., February 1996.

Rivest:1996:PMTa

[RS96b] R. Rivest and A. Shamir. PayWord and MicroMint — two simple micropayment schemes. Published in [RS96c]., April 1996. URL `http://theory.lcs.mit.edu/~rivest`.

Rivest:1996:PMTb

[RS96c] Ronald L. Rivest and Adi Shamir. Payword and MicroMint: Two simple micropayment schemes. *CryptoBytes*, 2(1):7–11, Spring 1996. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto2n1.pdf`. See [RS96b].

Reiter:1998:RAU

[RS98a] M. K. Reiter and S. G. Stubblebine. Resilient authentication using path independence. *IEEE Transactions on Computers*, 47(12): 1351–1362, December 1998. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=737682`.

Riordan:1998:CMP

[RS98b] J. Riordan and B. Schneier. A certified E-mail protocol with no trusted third party. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. URL `http://www.counterpane.com/certified-email.html`. 13th Annual Computer Security Applications Conference, ACM Press, December 1998, to appear.

Riordan:1998:EKGa

[RS98c] J. Riordan and B. Schneier. Environmental key generation towards clueless agents. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. URL `http://www.counterpane.com/clueless-agents.html`. Also published in *Mobile Agents and Security*, G. Vigna, ed., Springer-Verlag, 1998, pp. 15–24 [RS98d].

Riordan:1998:EKGb

[RS98d] J. Riordan and B. Schneier. Environmental key generation towards clueless agents. *Lecture Notes in Computer Science*, 1419: 15–24, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.counterpane.com/clueless-agents.html`. See [RS98c].

Rivest:1998:SPN

[RS98e] Ronald L. Rivest and

Robert D. Silverman. Are ‘strong’ primes need for RSA? Technical report, RSA Data Security, Inc., Redwood City, CA, USA, December 1, 1998. 22 pp. URL ftp://ftp.rsasecurity.com/pub/pdfs/sp2.pdf; ftp://ftp.rsasecurity.com/pub/ps/sp2.ps.

Ryan:1998:ARA

[RS98f] P. Y. A. Ryan and S. A. Schneider. An attack on a recursive authentication protocol — a cautionary tale. *Information Processing Letters*, 65(1):7–10, January 15, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ravi:1999:AAT

[RS99a] R. Ravi and F. S. Salman. Approximation algorithms for the traveling purchaser problem and its variants in network design. *Lecture Notes in Computer Science*, 1643:29–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Reiter:1999:AMA

[RS99b] Michael K. Reiter and Stuart G. Stubblebine. Authentication metric analysis and design. *ACM Transactions on Information and System Security*, 2(2):138–158, May 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org/pubs/citations/journals/tissec/1999-2-2/p138-reiter/.

Roeckl:1999:CPS

[RS99c] C. Roeckl and D. Sangiorgi. A λ-calculus process semantics of concurrent idealised ALGOL. *Lecture Notes in Computer Science*, 1578:306–321, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rozenberg:1999:DCN

[RS99d] G. Rozenberg and A. Salomaa. DNA computing: New ideas and paradigms. *Lecture Notes in Computer Science*, 1644:106–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rivest:19xx:SPN

[RSxx] R. L. Rivest and R. D. Silverman. Are strong primes needed for RSA? To appear., 19xx.

Rivest:1978:MOD

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of* *the Association for Computing Machinery*, 21(2): 120–126, February 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). The basics of trap-door functions and the famous RSA public key cryptosystem are presented in this paper.

Rivest:1982:MOD

[RSA82] Ronald Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public key cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 217–239. Westview, Boulder, CO, 1982.

Rivest:1983:MOD

[RSA83] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the Association for Computing Machinery*, 26 (1):96–99, January 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

RSA:1993:PRE

[RSA93a] RSA Laboratories. *PKCS #1: RSA Encryption Standard, Version 1.5.* RSA Data Security, Inc., Redwood City, CA, USA, November 1993. ?? pp. URL `http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html`.

RSA:1993:PDH

[RSA93b] RSA Laboratories. *PKCS #3: Diffie–Hellman Key-Agreement Standard*. RSA Data Security, Inc., Redwood City, CA, USA, November 1, 1993. URL `http://www.rsasecurity.com/rsalabs/pkcs/pkcs-3/index.html`.

RSA:1993:PEC

[RSA93c] RSA Laboratories. *PKCS #6: Extended-Certificate Syntax Standard*. RSA Data Security, Inc., Redwood City, CA, USA, November 1, 1993. URL `http://www.rsasecurity.com/rsalabs/pkcs/pkcs-6/index.html`.

RSA:1993:PCM

[RSA93d] RSA Laboratories. *PKCS #7: Cryptographic Message Syntax Standard*. RSA Data Security, Inc., Redwood City, CA, USA, November 1, 1993. URL `http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html`.

RSA:1993:PPK

[RSA93e] RSA Laboratories. *PKCS #8: Private-Key Information Syntax Standard*. RSA Data Security, Inc., Redwood City, CA, USA, November 1, 1993. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-8/index.html.

Laboratories:1993:PKC

[RSA93f] RSA Laboratories. *Public Key Cryptography Standard #1: RSA Encryption Standard Version 1.5.* RSA Data Security, Inc., Redwood City, CA, USA, November 1993. ?? pp.

RSA:1994:MPK

[RSA94] RSA. *MailSafe: Public Key Encryption Software (user's manual), Version 5.0.* RSA Data Security, Inc., Redwood City, CA, USA, 1994.

RSA:1999:PVPb

[RSA99a] RSA Laboratories. *PKCS #12 v1.0: Personal Information Exchange Syntax.* RSA Data Security, Inc., Redwood City, CA, USA, June 24, 1999. 23 pp. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/index.html.

RSA:1999:PVPa

[RSA99b] RSA Laboratories. *PKCS #5 v2.0: Password-Based Cryptography Standard.* RSA Data Security, Inc., Redwood City, CA, USA, March 25, 1999. 30 pp. URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-5/index.html.

Reed:1998:ACO

[RSG98] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, 16(4):482–494, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072144.html.

Reif:1988:EPP

[RT88] J. H. Reif and J. D. Tygar. Efficient parallel pseudorandom number generation. *SIAM Journal on Computing*, 17(2):404–411, ???? 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Rezny:1993:BCM

[RT93] M. Rezny and E. Trimarchi. A block cipher method using combinations of different methods under the control of the user key. *Lecture Notes in Computer Science*, 718:531–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Raleigh:1988:CDP

[RU88] T. M. Raleigh and R. W. Underwood. CRACK: a distributed password advisor. In USENIX [USE88a], pages 12–13. LCCN QA76.8.U65 U55 1988(1)-1990(2)//. Abstract only.

Rubin:1979:DSC

[Rub79] F. Rubin. Decrypting a stream cipher based on J–K flip-flops. *IEEE Transactions on Computers*, C-28(7):483–487, July 1979. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1675392`.

Rudolph:1982:HTI

[Rud82] James G. Rudolph, editor. *High technology in the information industry: digest of papers/Compcon spring 82, February 22–25; twenty-fourth IEEE computer society international conference, Jack Tar Hotel, San Francisco, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982. ISBN ???? LCCN TK7885.A1 C53 1982. IEEE catalog number 82CH1739-2.

Rudich:1991:UIP

[Rud91] Steven Rudich. The use of interaction in public cryptosystems (extended abstract). *Lecture Notes in Computer Science*, 576: 242–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760242.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760242.pdf`.

Rueppel:1993:ACE

[Rue93] Rainer A. Rueppel, editor. *Advances in cryptology — EUROCRYPT '92: Workshop on the Theory and Application of Cryptographic Techniques, Balatonfured, Hungary, May 24–28, 1992: proceedings*, volume 658 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. CODEN LNCSD9. ISBN 0-387-56413-6 (New York), 3-540-56413-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1992.

Rueppel:1998:E

[Rue98] R. A. Rueppel. Eurocrypt '92. *Lecture Notes in Computer Science*, 1440: 141–146, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ruggiu:1985:CCT

[Rug85] G. Ruggiu. Cryptology and complexity theories. In Beth et al. [BCI85], pages 3–9. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0209.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=209. Held at the University of Paris, Sorbonne.

Ruohonen:1994:EDO

[Ruo94] K. Ruohonen. Event detection for ODEs and nonrecursive hierarchies. *Lecture Notes in Computer Science*, 812:358–371, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Russell:1927:CMS

[Rus27] Henry Norris Russell. Cipher messages of the stars. *Scientific American*, 137 (2):118–119, August 1927. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v137/n2/pdf/scientificamerican0827-118.pdf.

Russel:1990:HLS

[Rus90] D. Russel. High-level security architecture and the Kerberos system. *Computer Networks and ISDN Systems*, 19(??):201–214, 1990. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic).

Ruskey:1993:SCG

[Rus93a] F. Ruskey. Simple combinatorial gray codes constructed by reversing sublists. *Lecture Notes in Computer Science*, 762:201–208, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Russell:1993:NSC

[Rus93b] A. Y. Russell. Necessary and sufficient conditions for collision-free hashing. *Lecture Notes in Computer Science*, 740:433–441, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Roychowdhury:1999:ENQ

[RV99] V. P. Roychowdhury and F. Vatan. On the existence of nonadditive quantum codes. *Lecture Notes in Computer Science*, 1509: 325–336, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Reeds:1984:FSU

[RW84] James A. Reeds and Peter J. Weinberger. File security and the UNIX system `crypt` command. *ATT Bell*

Lab. tech. j, 63(8 part 2): 1673–1683, October 1984. CODEN ABLJER. ISSN 0748-612X (print), 2376-7162 (electronic). Reprinted in [AT&T86, pp. 93–103].

Robshaw:1997:ECC

[RY97] M. J. B. Robshaw and Yiqun Lisa Yin. Elliptic curve cryptosystems. Technical report, RSA Data Security, Inc., Redwood City, CA, USA, June 27, 1997. URL `http://www.rsasecurity.com/rsalabs/ecc/elliptic_curve.html`.

Rytter:1986:SCU

[Ryt86] Wojciech Rytter. The space complexity of the unique decipherability problem. *Information Processing Letters*, 23(1):1–3, July 20, 1986. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ras:1999:DES

[RZ99] Z. W. Ras and J. M. Zytkow. Discovery of equations and the shared operational semantics in distributed autonomous databases. *Lecture Notes in Computer Science*, 1574: 453–463, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

S:1873:COD

[S.73] H. S. *Cryptographie, ou, Divers systèmes d'écrire secrète spécialement pour l'usage des cartes postales: combinations alphabétiques, correspondance chiffrée, écriture par signes: divers procédés pour la fabrication d'encres sympathiques.* G. Jousset, Paris, France, 1873. 8 pp. LCCN Z104 .H16 1873.

Schiller:1995:SWT

[SA95] Jeffrey I. Schiller and Derek Atkins. Scaling the web of trust: Combining Kerberos and PGP to provide large scale authentication. In USENIX Association [USE95a], pages 83–94. ISBN 1-880446-67-7. LCCN QA 76.76 O63 U88 1995. URL `http://www.usenix.org/publications/library/proceedings/neworl/index.html`.

Sabourin:1994:CCP

[Sab94] Conrad F. Sabourin. *Computational character processing: character coding, input, output, synthesis, ordering, conversion, text compression, encryption, display hashing, literate programming : bibliography.* Infolingua, Montréal, PQ, Canada, 1994. ISBN 2-921173-18-2. vii + 579 pp. LCCN ????

Sacco:1936:MC

[Sac36] Luigi Sacco. *Manuale di crittografia. (Italian) [Manual of cryptography]*. Tipografia Santa Barbara, Roma, Italia, second edition, 1936. viii + 247 + 8 pp.

Sacco:1947:MC

[Sac47] Luigi Sacco. *Manuale di crittografia. (Italian) [Manual of cryptography]*. Istituto Polygrafico Dello Stato, Roma, Italia, third edition, 1947. xii + 374 pp.

Sacco:1951:MCF

[Sac51] Luigi Sacco. *Manuel de cryptographie. (French) [Manual of cryptography]*. Payot, Paris, France, 1951. ???? pp.

Sacco:1977:MC

[Sac77] Luigi Sacco. *Manual of cryptography*, volume 14 of *A Cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1977. ISBN 0-89412-016-6. x + 193 pp. LCCN Z104 .S313 1977. Translation of: Manuale di crittografia. Bibliography: p. viii.

Sahai:1999:NMN

[Sah99] A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In IEEE [IEE99a], pages 543–553. CODEN ASFPDV. ISBN 0-7695-0409-4 (softbound), 0-7803-5955-0 (casebound), 0-7695-0411-6 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1999. IEEE Catalog Number 99CB37039.

Saks:1989:RNP

[Sak89] Michael Saks. A robust noncryptographic protocol for collective coin flipping. *SIAM Journal on Discrete Mathematics*, 2(2):240–244, May 1989. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Sakurai:1996:HCA

[Sak96] K. Sakurai. A hidden cryptographic assumption in no-transferable identification schemes. *Lecture Notes in Computer Science*, 1163: 159–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sakurai:1997:PPK

[Sak97] Kouichi Sakurai. Practical proofs of knowledge without relying on theoretical proofs of membership on languages. *Theoretical Computer Science*, 181(2): 317–335, July 30, 1997. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http:`

//www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1997&volume=181&issue=2&aid=2479.

Saltzer:1973:PCI

[Sal73] Jerome H. Saltzer. Protection and control of information sharing in Multics. *Operating Systems Review*, 7 (4):119, October 1973. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Saltzer:1978:DS

[Sal78] Jerome H. Saltzer. On digital signatures. *Operating Systems Review*, 12(2):12–14, April 1978. CODEN OSRED8. ISSN 0163-5980.

Salomaa:1985:PKC

[Sal85] Arto Salomaa. On a public-key cryptosystem based on parallel rewriting. In *Parcella '84 (Berlin, 1984)*, volume 25 of *Math. Res.*, pages 209–214. Akademie-Verlag, Berlin, 1985.

Salomaa:1988:PKC

[Sal88] Arto Salomaa. A public-key cryptosystem based on language theory. *Computers and Security*, 7(1):83–87, February 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488890507X.

Salomaa:1990:PC

[Sal90] Arto Salomaa. *Public-key cryptography*, volume 23 of *EATCS monographs on theoretical computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 3-540-52831-8 (Berlin), 0-387-52831-8 (New York). x + 245 pp. LCCN QA76.9.A25 S26 1990.

Salomaa:1991:VRS

[Sal91] A. Salomaa. Verifying and recasting secret ballots in computer networks. *Lecture Notes in Computer Science*, 555:283–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sale:1993:EBP

[Sal93] Tony Sale. The Enigma of Bletchley Park. *Resurrection: The Computer Conservation Society Journal*, ??(6):??, Summer 1993. ISSN 0958-7403. URL https://computerconservationsociety.org/resurrection/res06.htm#e.

Salomaa:1996:PC

[Sal96] Arto Salomaa. *Public-key cryptography*. Texts in theoretical computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second enlarged edition, 1996. ISBN 3-540-61356-0 (hardcover). x + 271 pp. LCCN QA76.9.A25 S26 1996.

Salvail:1998:QBC

[Sal98] L. Salvail. Quantum bit commitment from a physical assumption. *Lecture Notes in Computer Science*, 1462:338–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Salvail:1999:SHG

[Sal99] L. Salvail. The search for the Holy Grail in quantum cryptography. *Lecture Notes in Computer Science*, 1561:183–216, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shimoyama:1997:IFS

[SAM97] T. Shimoyama, S. Amada, and S. Moriai. Improved fast software implementation of block ciphers. *Lecture Notes in Computer Science*, 1334:269–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sameshima:1998:KES

[Sam98] Y. Sameshima. A key escrow system of the RSA cryptosystem. *Lecture Notes in Computer Science*, 1396:135–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sansom:1986:BRC

[San86] Robert Sansom. Book review: *Computer Security: A Global Challenge — Proceedings of the Second IFIP International Conference on Computer Security, IFIP/Sec'84, Toronto, Ontario, Canada, 10–12 September, 1984*: (Elsevier Science Publishing Co. 1984). *Operating Systems Review*, 20(3):9, July 1986. CODEN OSRED8. ISSN 0163-5980.

Sandhu:1988:CIT

[San88] Ravinderpal S. Sandhu. Cryptographic implementation of a tree hierarchy for access control. *Information Processing Letters*, 27(2): 95–98, February 29, 1988. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sarton:1928:BRBn

[Sar28] George Sarton. Book review: *The Cipher of Roger Bacon* by William Romaine Newbold; Roland Grubb Kent. *Isis*, 11(1):141–145, September 1928. CODEN ISISA4. ISSN 0021-1753 (print), 1545-6994 (electronic). URL `http://www.jstor.org/stable/224770`.

Sars:1997:STL

[Sar97] Camillo Sars. The SSH Transport Layer Protocol: Making the Internet secure. *Dr. Dobb's Journal of Software Tools*, 22(10):38, 40, 42–43, October 1997. CODEN DDJOEB. ISSN 1044-789X.

Sargent:1999:FID

[Sar99] P. Sargent. Feature identities, descriptors and handles. *Lecture Notes in Computer Science*, 1580:41–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sasaki:1999:SFU

[Sas99a] Ryoichi Sasaki. Secure fingerprinting using public-key cryptography (transcript of discussion). *Lecture Notes in Computer Science*, 1550:90–94, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1550/15500090.htm; http://link.springer-ny.com/link/service/series/0558/papers/1550/15500090.pdf.

Swierstra:1999:DIC

[SAS99b] S. D. Swierstra, P. R. A. Alcocer, and J. Saraiva. Designing and implementing combinator languages. *Lecture Notes in Computer Science*, 1608:150–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Satyanarayanan:1989:ISL

[Sat89] M. Satyanarayanan. Integrating security in a large distributed system. *ACM Transactions on Computer Systems*, 7(3):247–280, August 1989. CODEN ACSYEC. ISSN 0734-2071. URL http://www.acm.org:80/pubs/citations/journals/tocs/1989-7-3/p247-satyanarayanan/.

Saunders:1989:IDE

[Sau89] Barry Ferguson Saunders. Insection and decryption: Edgar Poe's *The gold bug* and the diagnostic gaze. Thesis (M.A.), University of North Carolina at Chapel Hill, Chapel Hill, NC, USA, 1989. x + 116 pp.

Savarnejad:1996:COF

[Sav96] Atoosa Savarnejad. Cisco offers free encryption technology. *Network Security*, 1996(5):4–5, May 1996. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485896901130.

Savarnejad:1997:GAD

[Sav97] Atoosa Savarnejad. Group asks for disclosure of travel records of crypto czar. *Network Security*, 1997(7):8–9, July 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897898789.

Sawirudin:1955:PND

[Saw55] Sawirudin. *Pegawai negeri dan PGP baru*. Badan Penerbitan Dewan Nasional SOBSI, Djakarta, cet. 1. edition, 1955. 93 pp.

Schaumuller-Bichl:1982:ADE

[SB82] Ingrid Schaumuller-Bichl. *Zur Analyse des Data Encryption: Standard und Synthese verwandter Chiffriersysteme*. PhD thesis, Johannes Kepler-Universität Linz, Linz, Austria, 1982. 168 pp. Summary in English. Published by VWGO, Wien, Austria.

Sorkin:1984:MCC

[SB84] Arthur Sorkin and C. James Buchanan. Measurement of cryptographic capability protection algorithms. *Computers and Security*, 3(2):101–116, May 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488490052X.

Smid:1992:DES

[SB92] Miles E. Smid and Dennis K. Branstad. The Data Encryption Standard: Past and future. In Simmons [Sim92], chapter 1, pages 43–64. ISBN 0-87942-277-7. LCCN QA76.9.A25 C6678 1992. US$79.95. IEEE order number: PC0271-7.

Smid:1993:RCN

[SB93] Miles E. Smid and Dennis K. Branstad. Response to comments on the NIST proposed digital signature standard (invited). *Lecture Notes in Computer Science*, 740:76–88, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0740/07400076.htm; http://link.springer-ny.com/link/service/series/0558/papers/0740/07400076.pdf.

Shepherd:1994:UBS

[SB94] S. J. Shepherd and S. K. Barton. The use of Blum sequences as secure spreading codes. In ????, editor, *IEE Colloquium on Spread Spectrum Techniques for Radio Communications Systems, Savoy Place, London, 15 April 1994*, volume 1994/098, pages 8/1–8/6. IEE, London, UK, 1994. ISBN ???? LCCN ????

Shepherd:1995:CNL

[SB95] S. J. Shepherd and S. N. Blackler. Characterisation of non-linearity in block ciphers. In ????, editor, *Selected Papers from the Third International Symposium on Communication Theory and Applications, 10–14 July 1995, Ambleside, UK*, pages 307–315. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1995. ISBN ???? LCCN ????

Schneier:1997:EPP

[SB97] Bruce Schneier and David Banisar, editors. *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*. John Wiley and Sons, Inc., New York, NY, USA, August 1997. ISBN 0-471-12297-1. xvii + 747 pp. LCCN JC596.2.U5E44 1997. US$59.99. URL http://www.counterpane.com/privacy.html; http://www.wiley.com/compbooks/catalog/12297-1.htm.

Shi:1998:FMV

[SB98] C. Shi and B. Bhargava. A fast MPEG video encryption algorithm. In Effelsberg and Smith [ES98], pages 81–88. ISBN 1-58113-036-8. LCCN QA76.575.A36 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073169.html. ACM order number 43398.

Soto:1999:RTA

[SB99] Juan Soto and Lawrence Bassham. Randomness testing of the Advanced Encryption Standard candidate algorithms. NIST internal report 6390, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 1999. 14 pp. URL http://csrc.nist.gov/rng/AES-REPORT2.doc. September.

Serpell:1985:PES

[SBC85] S. C. Serpell, C. B. Brookson, and B. L. Clark. A prototype encryption system using public key. In Blakley and Chaum [BC85], pages 3–9. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=3. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Smillie:1985:RFM

[SBET85] K. W. Smillie, F. L. Bauer, Ralph Erskine, and Henry S. Tropp. Reviews: O. I. Franksen, Mr. Babbage's Secret; F. H. Hinsley, British Intelligence in the Second World War; T. M. Thompson, From Error-Correcting Codes Through Sphere Packings to Simple Groups; capsule reviews. *Annals of the History of Computing*, 7(2):185–191, April/June 1985. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1985/pdf/a2185.pdf; http://www.computer.org/annals/an1985/a2185abs.htm.

Stallmann:1999:HED

[SBG99] M. Stallmann, F. Brglez, and D. Gosh. Heuristics and experimental design for bigraph crossing number minimization. *Lecture Notes in Computer Science*, 1619:74–93, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sicgberg:1999:TDG

[SBGK99] A. Sicgberg, A. Bredenfeld, H. Guenther, and H. U. Kobialka. Team description of the GMD RoboCup-Team. *Lecture Notes in Computer Science*, 1604:473–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sztandera:1999:ANN

[SBTV99] L. M. Sztandera, C. Bock, M. Trachtman, and J. Velga. Artificial neural networks aid the design of non-carcinogenic azo dyes. *Lecture Notes in Computer Science*, 1609:503–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shepherd:1999:NCS

[SBVG99] S. J. Shepherd, S. N. Blackler, P. W. J. Van Eetvelt, and D. A. Gillies. On the 2-nongroup and its cryptographic significance. *SIAM Journal on Discrete Mathematics*, ??(??): ??, ???? 1999. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic). Submitted, but apparently never published in this journal (as of 24 August 2011).

Chen:1985:RGE

[sC85] Su shing Chen. On rotation group and encryption of analog signals. In Blakley and Chaum [BC85], pages 95–100. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http:/

/www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=95. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Schneider:1996:RCB

[SC96a] M. Schneider and S. F. Chang. A robust content based digital signature for image authentication. In IEEE [IEE96e], pages 227–230. ISBN 0-7803-3258-X (softbound), 0-7803-3259-8 (casebound), 0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM). LCCN TK8315.I222 1996. Three volumes. IEEE catalog number 96CH35919.

Smith:1996:MIH

[SC96b] J. R. Smith and B. O. Comiskey. Modulation and information hiding in images. In Anderson [And96c], pages 207–226. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054163.html.

Sun:1997:DCP

[SC97] H.-M. Sun and B.-L. Chen. On the decomposition constructions for perfect secret sharing schemes. *Lecture Notes in Computer Science*, 1334:50–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schneider:19xx:DWI

[SCxx] M. Schneider and S.-F. Chang. Digital watermarking and image authentication. Technical Report ??, Columbia University, New York, NY, USA, ???? 19xx. ??–?? pp.

Scacchitti:1986:CT

[Sca86] Fred A. Scacchitti. The cryptographer's toolbox. *Dr. Dobb's Journal of Software Tools*, 11(5):58–??, May 1986. CODEN DDJOEB. ISSN 1044-789X.

Styner:1999:BMD

[SCG99] M. Styner, T. Coradi, and G. Gerig. Brain morphometry by distance measurement in a non-Euclidean, curvilinear space. *Lecture Notes in Computer Science*, 1613:364–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schwenter:1620:SSN

[Sch20] Daniel Schwenter. *Steganologia & steganographia nova:*

Geheime magische, naturliche Red vnd Schreibkunst, einem in der nahe vnd ferrne Alsbalden oder in gewiser Zeit, so woln in Schimpff als Ernst, etwas verborgens vnnd geheimes zu eroffnen durch Reden, Schreiben vnd mancherley Instrumenta: item wie verborgene Schrifften zu machen, auffzulosen, vnd mit sonderlichen Kunsten zu schreiben. Resene Gibronte Runeclus Hanedi, Nürnberg, Germany, 1620. 16 + 299 + 5 pp. LCCN KK276 .E36 1575; Z103.5. Publication year uncertain. Publicirt vnd an Tag gegeben durch Resene Gibronte Runeclus Hanedi ... Nurnberg: Inn Verlegung Simon Halbmayers.

Schwenter:1633:SSA

[Sch33] Daniel Schwenter. *Steganologia & [i.e. et] steganographia aucta: geheime, magische, naturliche Red vnnd Schreibkunst.* Resene Gibronte Runeclusam Hunidem, Nürnberg, Germany, 1633. 24 + 370 pp. LCCN Z103 .S38 1633. Auffs neue revidirt, an etlichen Orten corrigirt, ... augirt, vnd dann zum drittenmal in Truck verfertiget durch Janum Herculem de Sunde, sonst Resene Gibronte Runeclusam Hunidem .... Nurnberg, In Verlegung Jeremiae Dumlers [between 1633 and 1636].

Schroeder:1969:IC

[Sch69] M. R. Schroeder. Images from computers. *IEEE Spectrum*, 6(3):66–78, March 1969. CODEN IEESAM. ISSN 1939-9340.

Schroeder:1975:ESK

[Sch75] Michael D. Schroeder. Engineering a security kernel for Multics. *Operating Systems Review*, 9(5):25–32, November 1975. CODEN OSRED8. ISSN 0163-5980.

Schell:1983:SPA

[Sch83] K. J. Schell. Security printers application of lasers. *Proceedings of SPIE — The International Society for Optical Engineering*, 396: 131–140, 1983. CODEN PSISDG. ISBN 0-89252-431-6. ISSN 0277-786X (print), 1996-756X (electronic).

Schroeder:1984:NTS

[Sch84] M. R. (Manfred Robert) Schroeder. *Number theory in science and communication: with applications in cryptography, physics, biology, digital information, and computing*, volume 7 of *Springer series in information sciences.* Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1984. ISBN

0-387-12164-1. xvi + 324 pp. LCCN QA241 .S318 1984.

Schroeder:1986:NTS

[Sch86] M. R. (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., second enlarged edition, 1986. ISBN 0-387-15800-6. xix + 374 pp. LCCN QA241 .S3181 1986.

Schnorr:1990:EISb

[Sch90a] C. Schnorr. Efficient identification and signatures for smartcards. In Brassard [Bra90c], pages 239–252. CODEN LNCSD9. ISBN 0-387-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435`. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Schnorr:1990:EISa

[Sch90b] Claus P. Schnorr. Efficient identification and signatures for smart cards (abstract). *Lecture Notes in Computer Science*, 434: 688–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340688.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340688.pdf`.

Schroeder:1990:NTS

[Sch90c] M. R. (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., second enlarged, corrected printing edition, 1990. ISBN 0-387-15800-6. xix + 374 pp. LCCN QA 241 S318 1990.

Schmitt:1991:EAA

[Sch91a] Joacheim Schmitt. An embedding algorithm for algebraic congruence function fields. In Watt [Wat91], pages 187–188. ISBN 0-

89791-437-6. LCCN QA 76.95 I59 1991. URL http://www.acm.org:80/pubs/citations/proceedings/issac/120694/p187-schmitt/.

Schneier:1991:OHF

[Sch91b] Bruce Schneier. One-way hash functions: Probabilistic algorithms can be used for general-purpose pattern matching. *Dr. Dobb's Journal of Software Tools*, 16 (9):148–151, September 1, 1991. CODEN DDJOEB. ISSN 1044-789X.

Schnorr:1991:FHE

[Sch91c] C. P. Schnorr. FFT-hashing, an efficient cryptographic hash function. In Feigenbaum [Fei91], page ?? CODEN LNCSD9. ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1991. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0576.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=576. Conference held Aug. 11–15, 1991, at the University of California, Santa Barbara.

Schifreen:1992:PPD

[Sch92a] R. Schifreen. Practical PC data security. *BYTE Magazine*, 17(8):94IS–23–24, 94IS–26, 94IS–28, 94IS–30, August 1992. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Schneier:1992:SSA

[Sch92b] Bruce Schneier. Sharing secrets among friends. *Computer Language Magazine*, 9 (4):57–??, April 1992. CODEN COMLEF. ISSN 0749-2839.

Schneier:1992:UPC

[Sch92c] Bruce Schneier. Untangling public-key cryptography: the key to secure communications. *Dr. Dobb's Journal of Software Tools*, 17(5):16, 17, 20, 22, 24, 26, 28, May 1992. CODEN DDJOEB. ISSN 1044-789X.

Schilling:1993:MBC

[Sch93a] Donald L. Schilling, editor. *Meteor burst communications: theory and practice*. Wiley series in telecommunications. Wiley, New York, 1993. ISBN 0-471-52212-0. xi + 459 pp. LCCN TK6562.S5 S35 1993. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1011.html.

Schneier:1993:SCD

[Sch93b] B. Schneier. Subliminal channels in the Digital Signature Algorithm. *Computer Security Journal*, 9 (2):57–63, Fall 1993. CO-

DEN CSJLDR. ISSN 0277-0865. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/031624.html.

Schneier:1993:DS

[Sch93c] Bruce Schneier. Digital signatures. *BYTE Magazine*, 18(??):??, ?? 1993. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Schneier:1993:IEA

[Sch93d] Bruce Schneier. The IDEA encryption algorithm. *Dr. Dobb's Journal of Software Tools*, 18(13):50, 52, 54, 56, 106, December 1993. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1993:UHD

[Sch93e] Bruce Schneier. Under the hood: Digital signatures: Digital signatures will enable electronic documents to serve as legal instruments. *BYTE Magazine*, 18(12):3309–??, November 1993. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Schnorr:1993:FHI

[Sch93f] C. P. Schnorr. FFT-hash II, efficient cryptographic hashing. In Rueppel [Rue93], pages 41–51. CODEN LNCSD9. ISBN 0-387-56413-6 (New York), 3-540-56413-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1992.

Schnorr:1993:FIE

[Sch93g] C. P. Schnorr. FFT-hash II, efficient cryptographic hashing. *Lecture Notes in Computer Science*, 658: 45–54, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schiller:1994:SDC

[Sch94a] Jeffrey I. Schiller. Secure distributed computing. *Scientific American*, 271(5): 72–?? (Int. ed. 54–??), November 1994. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Schneier:1994:DNV

[Sch94b] B. Schneier. Description of a new variable-length key, 64-bit block cipher (Blowfish). *Lecture Notes in Computer Science*, 809: 191–204, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.counterpane.com/bfsverlag.html.

Schneier:1994:DEA

[Sch94c] B. Schneier. Designing encryption algorithms for real people. In *Proceedings of the 1994 ACM SIGSAC New Security Paradigms Workshop*, pages 63–71.

IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, August 1994. ISBN ???? LCCN ????

Schneier:1994:PAD

[Sch94d] B. Schneier. A primer on authentication and digital signatures. *Computer Security Journal*, 10(2):38–40, 1994. CODEN CSJLDR. ISSN 0277-0865.

Schneier:1994:SCD

[Sch94e] B. Schneier. Subliminal channels in the Digital Signature Algorithm. *PC Techniques*, 5(2):72–76, June 1994. CODEN ???? ISSN 1053-6205. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/032633.html.

Schneier:1994:AAd

[Sch94f] Bruce Schneier. Algorithm alley. *Dr. Dobb's Journal of Software Tools*, 19(13):113–??, November 1994. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1994:ACP

[Sch94g] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons, Inc., New York, NY, USA, 1994. ISBN 0-471-59756-2 (paperback). xviii + 618 pp. LCCN QA76.9.A25S35 1993. US$44.95.

Schneier:AC94

[Sch94h] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons, Inc., New York, NY, USA, 1994. ISBN 0-471-59756-2. xviii + 618 pp. LCCN QA76.9.A25S35 1993. US$44.95.

Schneier:1994:BEA

[Sch94i] Bruce Schneier. The Blowfish encryption algorithm. *Dr. Dobb's Journal of Software Tools*, 19(4):38, 40, 98, 99, April 1994. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1994:CAW

[Sch94j] Bruce Schneier. The Cambridge algorithms workshop. *Dr. Dobb's Journal of Software Tools*, 19(4):18–??, April 1994. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1994:NC

[Sch94k] Bruce Schneier. NP-completeness. *Dr. Dobb's Journal of Software Tools*, 19(10):119–121, September 1994. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1994:PYM

[Sch94l] Bruce Schneier. *Protect Your Macintosh*. Peachpit Press, Inc., 1085 Keith Avenue, Berkeley, CA 94708, USA, 1994. ISBN 1-56609-101-2. x + 315 pp. LCCN QA 76.9 A25 S35 1994. US$23.95. URL `http://www.peachpit.com/books/catalog/48436.html`. ... hands-on guide that discusses all aspects of Macintosh security: backups, viruses, data protection (including encryption), and physical security.

Schneier:1994:RDS

[Sch94m] Bruce Schneier. RSA data security conference. *Dr. Dobb's Developer Update*, 1 (4):3–??, April 1994. CODEN ???? ISSN 1079-8595.

Schneier:1995:AAB

[Sch95a] Bruce Schneier. Algorithm alley: The Blowfish encryption algorithm: One year later. *Dr. Dobb's Journal of Software Tools*, 20(9):137–??, September 1995. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1995:AAG

[Sch95b] Bruce Schneier. Algorithm alley: The GOST encryption algorithm. *Dr. Dobb's Journal of Software Tools*, 20(1):123–??, January 1995. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1995:MS

[Sch95c] Bruce Schneier. *E-Mail Security*. Ohmsha, Tokyo, Japan, 1995. ISBN 4-274-06117-5. 3500 yen. URL `http://www.counterpane.com/email-japanese.html`. Japanese translation of [Sch95d].

Schneier:1995:MSH

[Sch95d] Bruce Schneier. *E-Mail Security: how to keep your electronic messages private.* John Wiley and Sons, Inc., New York, NY, USA, 1995. ISBN 0-471-05318-X. xii + 365 pp. LCCN HE6239.E54 S36 1995. US$24.95. URL `http://www.counterpane.com/email.html`. Also available in Polish [Sch95e] and Japanese [Sch95c] editions.

Schneier:1995:OPE

[Sch95e] Bruce Schneier. *Ochrono Poczty Elektronicznej*. Wydawnictwa Naukowo-Techniczne, Warszawa, Poland, 1995. ISBN 83-204-1867-4. ???? pp. 280,000 zlotney. URL `http://www.counterpane.com/email-polish.html`. Polish translation of [Sch95d].

Schneier:1995:PCC

[Sch95f] Bruce Schneier. A pair of cryptographic conferences. *Dr. Dobb's Developer Update*, 2(3):3, March 1995. CODEN ???? ISSN 1079-8595.

Schneier:1996:ACP

[Sch96a] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source*

Code in C. John Wiley and Sons, Inc., New York, NY, USA, second edition, 1996. ISBN 0-471-12845-7 (hardcover), 0-471-11709-9 (paperback). xxiii + 758 pp. LCCN QA76.9.A25 S35 1996.

Schneier:1996:CC

[Sch96b] Bruce Schneier. Cryptography in the 21st Century. In USENIX [USE96f], page 352. ISBN 1-880446-76-6. LCCN QA 76.76 O63 U88 1996. URL `http://www.usenix.org/publications/library/proceedings/sd96/`. Unpublished invited talk.

Schneier:1996:DLC

[Sch96c] Bruce Schneier. Differential and linear cryptanalysis. *Dr. Dobb's Journal of Software Tools*, 21(1):42, 44, 46, 48, January 1996. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1997:IRC

[Sch97a] Bruce Schneier. Inside risks: Cryptography, security, and the future. *Communications of the Association for Computing Machinery*, 40 (1):138, January 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.counterpane.com/csf.html`.

Schneier:1997:WCH

[Sch97b] Bruce Schneier. Why cryptography is harder than it looks. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1997. 8 pp. URL `http://www.counterpane.com/whycrypto.html`.

Schroeder:1997:NTS

[Sch97c] M. R. (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., third edition, 1997. ISBN 3-540-62006-0. ISSN 0720-678X. xxii + 362 pp. LCCN QA241.S318 1997.

Schweighofer:1997:DIF

[Sch97d] E. Schweighofer. Downloading, information filtering and copyright. *Information & Communications Technology Law*, 6(2):??, June 1997. ISSN 1360-0834. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064383.html`.

Schlesinger:1998:CPC

[Sch98a] Stephen Schlesinger. Cryptanalysis for peacetime: codebreaking and the birth and structure of the United Nations. In Deavours et al. [DKK+98], pages 161–179. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL http://www.opengroup.com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Schmalz:1998:MDI

[Sch98b] Mark S. Schmalz, editor. *Mathematics of data/image coding, compression, and encryption: 21–22 July 1998, San Diego, California*, volume 3456 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 1998. ISBN 0-8194-2911-2. LCCN TA1637 .M38 1998; TA1637; TS510 .S63; TA1637 .M38 1998eb; Internet. URL http://link.spie.org/PSISDG/3456/1; http://uclibs.org/PID/38346.

Schneier:1998:CBT

[Sch98c] Bruce Schneier. The crypto bomb is ticking: Cracking encryption gets easier as computers get faster and cheaper. now what? *BYTE Magazine*, 23(5):97–??, May 1998. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Schneier:1998:CDV

[Sch98d] Bruce Schneier. Cryptographic design vulnerabilities. *Computer*, 31(9):29–33, September 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://computer.org/computer/r9029abs.htm; http://dlib.computer.org/co/books/co1998/pdf/r9029.pdf; http://www.counterpane.com/design-vulnerabilities.pdf.

Schneier:1998:CTS

[Sch98e] Bruce Schneier. Des chausses-trappes de sécurité en cryptologie. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. URL http://www.counterpane.com/pitfalls_french.html. French translation of [Sch98f].

Schneier:1998:SPC

[Sch98f] Bruce Schneier. Security pitfalls in cryptography. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. 11 pp. URL http://www.counterpane.com/pitfalls.html. Also available in French translation [Sch98e].

Schneier:1998:TEA

[Sch98g] Bruce Schneier. The Twofish encryption algorithm. *Dr. Dobb's Journal of Software Tools*, 23 (12):30, 32, 34, 36, 38, December 1998. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ddj/1998/1998_12/../../../ftp/1998/1998_12/twofish.zip.

Schoenmakers:1998:SAE

[Sch98h] B. Schoenmakers. Security aspects of the Ecash[TM] payment system. *Lecture Notes in Computer Science*, 1528:338–352, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schroeppel:1998:HPC

[Sch98i] Rich Schroeppel. The hasty pudding cipher — a tasty morsel. In National Institute of Standards and Technology [Nat98], page ?? ISBN ???? LCCN ???? URL http://www.cs.arizona.edu/~rcs/hpc/; http://www.cs.arizona.edu/~rcs/hpc/hpc-nist-doc; http://www.cs.arizona.edu/~rcs/hpc/hpc-oneyearlater; http://www.cs.arizona.edu/~rcs/hpc/hpc-ov-cl-hl-sp; http://www.cs.arizona.edu/~rcs/hpc/hpc-overview; http://www.cs.arizona.edu/~rcs/hpc/hpc-spec; http://www.cs.arizona.edu/~rcs/hpc/hpc-times-alpha.html; http://www.cs.arizona.edu/~rcs/hpc/hpc.hlp; http://www.cs.arizona.edu/~rcs/hpc/README; http://www.cs.arizona.edu/~rcs/hpc/README2; http://www.cs.arizona.edu/~rcs/hpc/test-index.html; http://www.cs.arizona.edu/~rcs/hpc/tweak. See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen "complete and proper" candidates.

Schaefer:1999:PES

[Sch99a] Ed Schaefer. Password encryption in shell scripts. *Sys Admin: The Journal for UNIX Systems Administrators*, 8(1):49–54, January 1999. CODEN SYADE7. ISSN 1061-2688. URL http://www.samag.com/.

Schmalz:1999:MDI

[Sch99b] Mark S. Schmalz, editor. *Mathematics of Data/Image Coding, Compression, and Encryption II: 19–20 July, 1999, Denver, Colorado*, volume 3814 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA,

USA, 1999. ISBN 0-8194-3300-4. LCCN TA1637 .M383 1999.

Schmidt:1999:RER

[Sch99c] D. A. Schmidt. A return to elegance: The reapplication of declarative notation to software design. *Lecture Notes in Computer Science*, 1551:360–364, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schneier:1999:SSC

[Sch99d] B. Schneier. Self-study course in block cipher cryptanalysis. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, January 3, 1999. 14 pp. URL `http://www.counterpane.com/self-study.html`.

Schneier:1999:IRR

[Sch99e] Bruce Schneier. Inside risks: Risks of relying on cryptography. *Communications of the Association for Computing Machinery*, 42(10): 144, October 1999. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/cacm/1999-42-10/p144-schneier/`.

Schneier:1999:IRT

[Sch99f] Bruce Schneier. Inside risks: the Trojan horse race. *Communications of the Association for Computing Machinery*, 42(9): 128, September 1999. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/cacm/1999-42-9/p128-schneier/`.

Schneier:1999:IRU

[Sch99g] Bruce Schneier. Inside risks: the uses and abuses of biometrics. *Communications of the Association for Computing Machinery*, 42(8): 136, August 1999. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/cacm/1999-42-8/p136-schneier/`.

Schneier:1999:IWC

[Sch99h] Bruce Schneier. Internet watch: Cryptography: The importance of not being different. *Computer*, 32(3): 108–109, March 1999. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co1999/pdf/r3108.pdf`.

Schoenmakers:1999:SPV

[Sch99i] B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In Wiener [Wie99], pages 148–164. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Schroeder:1999:SEA

[Sch99j] Wayne Schroeder. The SDSC encryption/authentication (SEA) system. *Concurrency: practice and experience*, 11(15):913–931, December 25, 1999. CODEN CPEXEI. ISSN 1040-3108. URL `http://www3.interscience.wiley.com/cgi-bin/abstract/71005732/START`; `http://www3.interscience.wiley.com/cgi-bin/fulltext?ID=71005732&PLACEBO=IE.pdf`.

Schumann:1999:PST

[Sch99k] J. Schumann. PIL/SETHEO: a tool for the automatic analysis of authentication protocols. *Lecture Notes in Computer Science*, 1633:500–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schwentick:1999:DCL

[Sch99l] T. Schwentick. Descriptive complexity, lower bounds and linear time. *Lecture Notes in Computer Science*, 1584:9–28, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Scerri:1999:UOS

[SCT99] P. Scerri, S. Coradeschi, and A. Toerne. A user oriented system for developing behavior based agents. *Lecture Notes in Computer Science*, 1604:173–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Scudder:1992:OLA

[Scu92] W. Blaine Scudder. *O. H. Lee/Alek James Hidell: a lesson in conspiracy and cryptology*. ????, ????, 1992. various pp.

Smith:1986:GCC

[SD86] G. W. Smith and J. B. H. Du Boulay. The generation of cryptic crossword clues. *The Computer Journal*, 29(3):282–284, June 1986. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Silvestre:1997:IWU

[SD97] G. C. M. Silvestre and W. J. Dowling. Image watermarking using digital communication techniques. In IEE [IEE97a], pages 443–447. CODEN IECPB4. ISBN 0-85296-692-X. ISSN 0537-9989. LCCN TK5.I4 no.443;

TA1632 .I553 1997. Two volumes.

Schouten:1999:FEU

[SD99] B. A. M. Schouten and P. M. De Zeeuw. Feature extraction using fractal codes. *Lecture Notes in Computer Science*, 1614:483–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sicherman:1983:AQR

[SDV83] George L. Sicherman, Wiebren De Jonge, and Reind P. Van De Riet. Answering queries without revealing secrets. *ACM Transactions on Database Systems*, 8(1): 41–59, March 1983. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL http://www.acm.org/pubs/articles/journals/tods/1983-8-1/p41-sicherman/p41-sicherman.pdf; http://www.acm.org/pubs/citations/journals/tods/1983-8-1/p41-sicherman/. Also published in/as: reprinted in deJonge thesis, Jun. 1985.

Smillie:1986:RWA

[SE86] K. W. Smillie and Ralph Erskine. Reviews: W. Aspray, Should the Term Fifth Generation Computers Be Banned?; C. A. Deavours and L. Kruh, Machine Cryptography and Modern Cryptanalysis; capsule reviews. *Annals of the History of Computing*, 8(2):199–200, 202, 204–205, April/June 1986. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1986/pdf/a2199.pdf; http://www.computer.org/annals/an1986/a2199abs.htm.

Schwenk:1996:PKE

[SE96] Jörg Schwenk and Jörg Eisfeld. Public key encryption and signature schemes based on polynomials over $\mathbf{Z}_n$. *Lecture Notes in Computer Science*, 1070: 60–71, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700060.htm; http://link.springer-ny.com/link/service/series/0558/papers/1070/10700060.pdf.

Seaton:1956:THS

[Sea56] E. Seaton. Thomas Hariot's secret script. *Ambix: Journal of the Society for the History of Alchemy and Chemistry*, 5(3–4): 111–114, 1956. CODEN AMBXAO. ISSN 0002-6980 (print), 1745-8234 (electronic). URL http://www.tandfonline.com/doi/abs/10.1179/amb.1956.5.3-4.111.

Sears:1986:SWK

[Sea86] Peter Sears. *Secret writing: keys to the mysteries of reading and writing*. Teachers and Writers Collaborative, New York, NY, USA, 1986. ISBN 0-915924-86-2 (paperback). xv + 160 pp. LCCN Z 103.3 S4 1986 Resources for Teaching–2nd Floor. US$9.95. Discusses secret writing, ciphers, and the processes of creating and deciphering secret or difficult languages. Includes thinking and writing exercises.

Seachrist:1995:DIM

[Sea95] D. Seachrist. Document image managers. *BYTE Magazine*, 20(5):143–144, 146, 148, 150, 152, May 1995. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Sedlak:1988:RCP

[Sed88] H. Sedlak. The RSA cryptographic processor: The first high speed one-chip solution. In Pomerance [Pom88], pages 95–105. CODEN LNCSD9. ISBN 0-387-18796-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1987; QA267.A1 L43 no.293. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0293.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=293`. CRYPTO '87, a Conference on the Theory and Applications of Cryptographic Techniques, held at the University of California, Santa Barbara ... August 16–20, 1987.

Sedgewick:1992:AC

[Sed92] Robert Sedgewick. *Algorithms in C++*. Addison-Wesley, Reading, MA, USA, 1992. ISBN 0-201-36118-3, 0-201-51059-6. xiv + 656 pp. LCCN QA76.73.C153 S38 1992.

Sedgewick:1993:AM

[Sed93] Robert Sedgewick. *Algorithms in Modula-3*. Addison-Wesley, Reading, MA, USA, 1993. ISBN 0-201-53351-0. xiv + 656 pp. LCCN QA76.73.M63 S43 1993.

Seeley:1989:PCG

[See89] Donn Seeley. Password cracking: a game of wits. *Communications of the Association for Computing Machinery*, 32(6):700–703, June 1989. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/63529.html`.

Seethamraju:1997:HII

[See97] Srisai Rao Seethamraju. A hardware implementation of the International Data Encryption Algorithm. Thesis (M.S.), North Carolina State University, Raleigh, NC, USA, 1997. 123 pp.

Segal:1992:NTC

[Seg92] Alida Segal. New trends in cryptology. Thesis (M.S. [C.Sc.]), School of Engineering. Department of Computer Sciences, City College of New York, New York, NY, USA, 1992. 3 + 34 pp.

Selmer:1994:MNC

[Sel94] E. Selmer. From the memoirs of a Norwegian cryptologist. *Lecture Notes in Computer Science*, 765: 142–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Selcuk:1998:NRL

[Sel98a] A. Aydin Selcuk. New results in linear cryptanalysis of RC5. *Lecture Notes in Computer Science*, 1372:1–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Selmer:1998:NMS

[Sel98b] Ernst S. Selmer. The Norwegian modification of the Siemens and Halske T52e cipher machines. In Deavours et al. [DKK+98], pages 461–463. ISBN 0-89006-862-3. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Serpell:1985:CES

[Ser85] S. C. Serpell. *Cryptographic equipment security: a code of practice*. Institution of Electronic and Radio Engineers, London, UK, 1985. ISBN 0-903748-62-2 (paperback). 25 pp. LCCN Z103.S47 1985.

Seshadri:1981:KPP

[Ses81] Raghavan Seshadri. Knapsack problems in public key encryption systems. Thesis (M.S.), University of Oklahoma, Norman, OK, USA, 1981. vii + 99 pp.

Sakurai:1997:ILC

[SF97] Kouichi Sakurai and Souichi Furuya. Improving linear cryptanalysis of LOKI91 by *Probabilistic Counting* method. *Lecture Notes in Computer Science*, 1267: 114–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670114.htm; http://link.springer-ny.com/link/service/series/`

0558/papers/1267/12670114.pdf.

Saglam:1995:ACL

[SG95] H. Saglam and J. P. Gallagher. Approximating constraint logic programs using polymorphic types and regular descriptions. *Lecture Notes in Computer Science*, 982:461–462, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shearer:1996:GCR

[SG96a] J. Shearer and P. Gutmann. Government, cryptography, and the right to privacy. *J.UCS: Journal of Universal Computer Science*, 2(3):113–??, March 28, 1996. ISSN 0948-6968. URL http://www.iicm.edu/government_cryptography_and_the_right_to_privacy.

Shieh:1996:DIL

[SG96b] Shiuh-Pyng Shieh and Virgil D. Gligor. Detecting illicit leakage of information in operating systems. *Journal of Computer Security*, 4(2–3):123–148, December 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061242.html.

Shoup:1998:STC

[SG98] Victor Shoup and Rosario Gennaro. Securing threshold cryptosystems against chosen ciphertext attack. *Lecture Notes in Computer Science*, 1403:1–16, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Saeednia:1999:SCG

[SG99a] S. Saeednia and H. Ghodosi. A self-certified group-oriented cryptosystem without a combiner. *Lecture Notes in Computer Science*, 1587:192–201, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sapir:1999:DRT

[SG99b] A. Sapir and E. Gudes. Dynamic relationships and their propagation and concurrency semantics in object-oriented databases. *Lecture Notes in Computer Science*, 1649:94–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sgarro:1990:IDB

[Sga90] Andrea Sgarro. Informational divergence bounds for authentication codes. *Lecture Notes in Computer Science*, 434:93–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349

(electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340093.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340093.pdf.

Sgarro:1991:STC

[Sga91a] A. Sgarro. A Shannon-theoretic coding theorem in authentication theory. *Lecture Notes in Computer Science*, 514:282–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sgarro:1991:LBA

[Sga91b] Andrea Sgarro. Lower bounds for authentication codes with splitting. *Lecture Notes in Computer Science*, 473:283–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730283.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730283.pdf.

Sgarro:1993:ITB

[Sga93] Andrea Sgarro. Information-theoretic bounds for authentication frauds. *Lecture Notes in Computer Science*, 658:467–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580467.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580467.pdf.

Slater:1998:CAD

[SGPV98] A. Slater, R. Gore, J. Posegga, and H. Vogt. cardT0AP: Automated deduction on a smart card. *Lecture Notes in Computer Science*, 1502: 239–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Syverson:1997:ACO

[SGR97] P. F. Syverson, D. M. Goldschlag, and M. G. Reed. Anonymous connections and onion routing. In IEEE [IEE97i], pages 44–54. ISBN 0-8186-7828-3 (softbound), 0-7803-4159-7 (casebound), 0-8186-7830-5 (microfiche). LCCN QA 76.9 A25 I43 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064452.html.

Simpson:1999:FCA

[SGSD99] L. Simpson, J. Golić, M. Salmasizadeh, and E. Dawson. A fast correlation attack on multiplexer generators. *Information Processing Letters*, 70

(2):89–93, April 30, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sun:1994:KGA

[SH94] Hung Min Sun and Tzone-lih Hwang. Key generation of algebraic-code cryptosystems. *Computers and Mathematics with Applications*, 27(2):99–106, 1994. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Schnorr:1995:ACC

[SH95a] C. P. Schnorr and H. H. Hoerner. Attacking the Chor–Rivest cryptosystem by improved lattice reduction. *Lecture Notes in Computer Science*, 921:1–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schnorr:1995:ACR

[SH95b] Claus P. Schnorr and H. H. Hörner. Attacking the Chor–Rivest cryptosystem by improved lattice reduction. *Lecture Notes in Computer Science*, 921: 1–12, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210001.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0921/09210001.pdf`.

Schneier:1997:IMS

[SH97] B. Schneier and C. Hall. An improved E-mail security protocol. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1997. URL `http://www.counterpane.com/e-mail_security_protocol.html`. Also published in *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 232–238.

Shi:1999:FGM

[SH99] Rong Hua Shi and Xiang Ling Hu. A fast generating method for keys of RSA cryptosystems. *Dianzi Keji Daxue Xuebao*, 28 (5):461–463, 1999. CODEN DKDAEM. ISSN 1001-0548.

Shannon:1945:MTC

[Sha45] Claude Shannon. A mathematical theory of cryptography. Classified report, Bell Laboratories, Murray Hill, NJ, USA, September 1, 1945.

Shannon:1948:MTCa

[Sha48a] Claude Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27 (3):379–423, July 1948. CODEN BSTJAN. ISSN 0005-

8580. From the first page: “If the base 2 is used the resulting units may be called binary digits, or more briefly, *bits*, a word suggested by J. W. Tukey.”. This is the first known printed instance of the word ‘bit’ with the meaning of binary digit.

Shannon:1948:MTCb

[Sha48b] Claude Shannon. A mathematical theory of communication (continued). *The Bell System Technical Journal*, 27(4):623–656, October 1948. CODEN BSTJAN. ISSN 0005-8580.

Shannon:1949:CTS

[Sha49] Claude Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28 (4):656–715, ???? 1949. CODEN BSTJAN. ISSN 0005-8580. URL `http://en.wikipedia.org/wiki/Communication_Theory_of_Secrecy_Systems; http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf`. A footnote on the initial page says: “The material in this paper appeared in a confidential report, ‘A Mathematical Theory of Cryptography’, dated Sept. 1, 1946, which has now been declassified.”.

Shamir:1979:HSS

[Sha79] Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11): 612–613, November 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Shamir:1982:PTA

[Sha82] Adi Shamir. A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem. In *23rd annual symposium on foundations of computer science (Chicago, Ill., 1982)*, pages 145–152. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982.

Shamir:1983:ECT

[Sha83a] Adi Shamir. Embedding cryptographic trapdoors in arbitrary knapsack systems. *Information Processing Letters*, 17(2):77–79, August 24, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shamir:1983:GCS

[Sha83b] Adi Shamir. On the generation of cryptographically strong pseudorandom sequences. *ACM Transactions on Computer Systems*, 1(1):38–44, February 1983. CODEN ACSYEC. ISSN

0734-2071 (print), 1557-7333 (electronic).

Shamir:1984:PTA

[Sha84] Adi Shamir. A polynomial-time algorithm for breaking the basic Merkle–Hellman cryptosystem. *IEEE Transactions on Information Theory*, 30(5):699–704, 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Shamir:1985:IBC

[Sha85] Adi Shamir. Identity-based cryptosystems and signature schemes. In Blakley and Chaum [BC85], pages 47–53. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=47`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Shamir:1986:SPS

[Sha86] A. Shamir. The search for provably secure identification schemes. In Gleason [Gle87], pages 1488–1495. ISBN 0-8218-0110-4. LCCN QA1 .I8 1986 v. 1-2. Two volumes.

Shamir:1987:CSS

[Sha87] Adi Shamir. Cryptography: State of the science. In Ashenhurst [Ash87], page ?? ISBN 0-201-07794-9. LCCN QA76.24 .A33 1987. ACM Turing Award lecture.

Sharp:1988:DCO

[Sha88] R. L. Sharp. Design of a certifiable one-way data-flow device. *AT&T Technical Journal*, 67(3):44–52, May 1988. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Shamir:1994:ESS

[Sha94] Adi Shamir. Efficient signature schemes based on birational permutations. *Lecture Notes in Computer Science*, 773:1–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shamir:1995:MEV

[Sha95a] Adi Shamir. Memory efficient variants of public-key schemes for smart card applications. *Lecture Notes in Computer Science*, 950: 445–449, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http:/`

/link.springer-ny.com/link/service/series/0558/bibs/0950/09500445.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500445.pdf.

Shamir:1995:RP

[Sha95b] Adi Shamir. RSA for paranoids. *CryptoBytes*, 1(3):1, 3–4, Autumn 1995. URL ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf.

Shaw:1997:VVA

[Sha97] Andrew Shaw. Voice verification — authenticating remote users over the telephone. *Network Security*, 1997(8):16–18, August 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897832412.

Shamir:1998:VC

[Sha98] A. Shamir. Visual cryptanalysis. *Lecture Notes in Computer Science*, 1403: 201–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shallit:1999:RHA

[Sha99a] Jeffrey Shallit. Reviews: *Handbook of Applied Cryptography*, by Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone; *The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet*, by Shawn James Rosenheim. *American Mathematical Monthly*, 106(1):??, January 1999. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Shamir:1999:PAK

[Sha99b] Adi Shamir. Power analysis of the key scheduling of the AES candidates. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Sherman:1986:CVT

[She86] Alan T. Sherman. *Cryptology and VLSI (a two-part dissertation). I, II, Detecting and exploiting algebraic weaknesses in cryptosystems. Algorithms for placing modules on a custom VLSI chip.* Thesis (Ph.D.), Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, October 1986. 221 pp.

Supervised by Ronald Linn Rivest.

Sherman:1987:CVT

[She87] Alan T. Sherman. *Cryptology and VLSI (a two-part dissertation). I, II, Detecting and exploiting algebraic weaknesses in cryptosystems. Algorithms for placing modules on a custom VLSI chip.* Thesis (Ph.D.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1987. 221 pp. Supervised by Ronald Linn Rivest.

Sherman:1988:CVV

[She88] A. T. Sherman. Cryptology and VLSI (Very Large Scale Integration). I. Detecting and exploiting algebraic weaknesses in cryptosystems. II. Algorithms for placing modules on a custom VLSI chip. *Computers and Security*, 7(5): 512, October 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404888902234`.

Shepherd:1992:DSA

[She92a] S. J. Shepherd. *A Distributed Security Architecture for Large Scale Systems.* Ph.D. thesis, University of Plymouth, Plymouth, UK, June 1992. ???? pp.

Shepherd:1992:FFW

[She92b] S. J. Shepherd. Factoring with false witnesses. Internal research note 1, Electronic and Electrical Engineering Department, University of Bradford, Bradford, Yorkshire, UK, February 1992.

Shepherd:1992:FHS

[She92c] S. J. Shepherd. A fast, high security public key processor. *Innovation Journal*, ?? (??):16–17, June 1992.

Shepherd:1992:HSC

[She92d] S. J. Shepherd. A high speed cryptographic engine. Internal Research Note 4, Electronic and Electrical Engineering Department, University of Bradford, Bradford, Yorkshire, UK, June 1992. Commercial-in-confidence.

Shepherd:1992:NPS

[She92e] S. J. Shepherd. A numerical processor with supercomputer performance based on state-of-the-art finite-impulse-response filter digital signal processors. Internal Research Note 5, Electronic and Electrical Engineering Department, University of Bradford, Bradford, Yorkshire, UK, October 1992. Commercial-in-confidence.

Shepherd:1992:SIR

[She92f] S. J. Shepherd. The security issues of radio LANs. In ????, editor, *Proceedings of the British Computer Society Special Interest Group Workshop on Computer Security, Solihull, 15 September 1992*, page ?? ????, ????, 1992. ISBN ???? LCCN ????

Sherrod:1992:DES

[She92g] Elizabeth Llewellyn Sherrod. Data Encryption Standard and Rivest-Shamir-Adleman encryption schemes: a comparative survey. Thesis (M.S.), Division of Computer Science, Department of Mathematical Sciences, Virginia Commonwealth University, Richmond, VA, USA, 1992. vi + 115 pp.

Shepherd:1993:ACCa

[She93a] S. J. Shepherd. Access control and cryptography. In ????, editor, *Proceedings of the First International Network Security Conference, London, 26–27 May 1993.*, page ?? ????, ????, 1993. ISBN ???? LCCN ????

Shepherd:1993:ACCb

[She93b] S. J. Shepherd. Access control and cryptography. In ????, editor, *Proceedings of the Fourth International PC Security Conference, London, 13–15 September 1993*, page ?? ????, ????, 1993. ISBN ???? LCCN ????

Shepherd:1993:EOS

[She93c] S. J. Shepherd. Extended OSI security architecture. In Muftic [Muf93], chapter 7–8, page ?? ISBN 0-471-93472-0. LCCN QA76.9.A25S376 1993.

Shepherd:1993:WNS

[She93d] S. J. Shepherd. Wireless network security and cryptography. In ????, editor, *Proceedings of the British Computer Society Computer Security Specialist Group, Sutton Coldfield, 13 March 1993*, page ?? ????, ????, 1993. ISBN ???? LCCN ????

Shepherd:1994:ACM

[She94a] S. J. Shepherd. An approach to the cryptanalysis of mobile stream ciphers. In ????, editor, *IEE Colloquium on Security and Cryptography Applications to Radio Systems, Digest No. 1994/141, Savoy Place, London, 3 June 1994*, page ?? ????, ????, 1994. ISBN ???? LCCN ???? Commercial-in-confidence.

Shepherd:1994:CGA

[She94b] S. J. Shepherd. Cryptanalysis of the GSM A5 cipher algorithm. In *IEE Colloquium on Security and Cryptography Applications to Ra-*

dio Systems, Savoy Place, London, 3 June 1994, volume 1994/141, page ?? IEE, London, UK, 1994. ISBN ???? LCCN ???? Commercial-in-confidence.

Shepherd:1994:MCM

[She94c] S. J. Shepherd. Multifunction coding and modulation for spread spectrum and CDMA with inherent security. In ????, editor, *Selected Papers from the IMA Conference on the Applications of Combinatorial Mathematics, 14–16 December 1994, Wadham College, Oxford*, page ?? Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1994. ISBN ???? LCCN ????

Shepherd:1994:PKS

[She94d] S. J. Shepherd. Public key stream ciphers. In ????, editor, *IEE Colloquium on Security and Cryptography Applications to Radio Systems, Savoy Place, London, 3 June 1994*, volume 1994/141, pages 10/1–10/7. IEE, London, UK, 1994. ISBN ???? LCCN ????

Shepherd:1995:CAA

[She95a] S. J. Shepherd. Continuous authentication by analysis of keyboard typing characteristics. In ????, editor, *Proceedings of the 1995 European Convention on Security and Detection (ECOS 95), Conf. Pub. 408, 16–18 May 1995, Brighton, UK*, page ?? ????, ????, 1995. ISBN ???? LCCN ????

Shepherd:1995:HSS

[She95b] S. J. Shepherd. A high speed software implementation of the Data Encryption Standard. *Journal of Computers and Security*, 14(4): 349–357, ???? 1995.

Shepherd:1995:PPH

[She95c] S. J. Shepherd. Primitive polynomials over GF(2) of Hamming weight 3 and 5 up to high order. Report 573, Electronic and Electrical Engineering Department, University of Bradford, Bradford, Yorkshire, UK, March 1995.

Shen:1996:APK

[She96a] Faming Shen. Automated public key encryption electronic mail facility. Thesis (M.S.), Department of Engineering Science, University of Toledo, Toledo, OH, USA, 1996. v + 67 pp.

Shepherd:1996:SWN

[She96b] S. J. Shepherd. Security weaknesses in the Netscape World Wide Web browser. In ????, editor, *IEE Colloquium on Public Uses of Cryptography, Savoy Place, London, 11 April 1996*, volume 96/085, pages 7/1–7/6. IEE, London, UK, 1996. ISBN ???? LCCN ????

Shecter:1997:SAD

[She97] Robb Shecter. Security and authentication with digital signatures. *Linux Journal*, 40:??, August 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Su:1998:GID

[SHG98] Jonathan K. Su, Frank Hartung, and Bernd Girod. Graphics in/for digital libraries — digital watermarking of text, image, and video documents. *Computers and Graphics*, 22(6):687–695, December 1, 1998. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.elsevier.com/cas/tree/store/cag/sub/1998/22/6/623.pdf.

Schneier:1999:TEAa

[SHK+99a] Bruce Schneier, Chris Hall, John Kelsey, David Wagner, and Doug Whiting. *The Twofish Encryption Algorithm*. John Wiley and Sons, Inc., New York, NY, USA, 1999. ISBN 0-387-98713-4. 200 pp. LCCN QA76.9.A25 T85 1999. US$29.95. URL http://www.springer-ny.com/compsci/catalog99/0-387-98713-4.html.

Smaus:1999:PIE

[SHK99b] J.-G. Smaus, P. Hill, and A. King. Preventing instantiation errors and loops for logic programs with multiple modes using block declarations. *Lecture Notes in Computer Science*, 1559: 289–307, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shoup:1996:FPS

[Sho96] Victor Shoup. On fast and provably secure message authentication based on universal hashing. *Lecture Notes in Computer Science*, 1109:313–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090313.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090313.pdf.

Shor:1997:PTA

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://

epubs.siam.org/sam-bin/dbq/article/29317.

Shparlinski:1999:FFT

[Shp99a] Igor E. Shparlinski. *Finite fields: theory and computation: the meeting point of number theory, computer science, coding theory, and cryptography*, volume 477 of *Mathematics and its applications*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1999. ISBN 0-7923-5662-4 (hb). xiv + 528 pp. LCCN QA247.3 .S477 1999.

Shparlinski:1999:NTM

[Shp99b] 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.

Shulman:1976:ABC

[Shu76] David Shulman. *An annotated bibliography of cryptography*, volume 37 of *Garland reference library of the humanities*. Garland Pub., New York, NY, USA, 1976. ISBN 0-8240-9974-5. 388 pp. LCCN Z103.A1 S58.

Shulman:1980:BRB

[Shu80a] David Shulman. Book review: *United States diplomatic codes and ciphers 1775–1938*: By Ralph E. Weber. Chicago. xviii + 633 pp. Illus. $49.95. *Historia Mathematica*, 7(4):452–454, November 1980. CODEN HIMADS. ISSN 0315-0860 (print), 1090-249X (electronic). URL http://www.sciencedirect.com/science/article/pii/0315086080900142.

Shulman:1980:BRU

[Shu80b] David Shulman. Book review: *United States diplomatic codes and ciphers 1775–1938*: By Ralph E. Weber. Chicago. xviii + 633 pp. Illus. $49.95. *Historia Mathematica*, 7(4):452–454, November 1980. CODEN HIMADS. ISSN 0315-0860 (print), 1090-249X (electronic). URL http://www.sciencedirect.com/science/article/pii/0315086080900142.

Shumaker:1982:RCJ

[Shu82] Wayne Shumaker. *Renaissance curiosa: John Dee's conversations with angels, Girolamo Cardano's horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno's Universal language*, volume 8 of *Medieval and Renaissance texts and studies*. Center for Medieval and

Early Renaissance Studies, Binghamton, NY, USA, 1982. ISBN 0-86698-014-8. 207 pp. LCCN CB361 .S494 1982. Intended audience: Renaissance specialists, linguistics, students of occultism, and historians of science.

Sakurai:1993:DBS

[SI93a] K. Sakurai and T. Itoh. On the discrepancy between serial and parallel of zero-knowledge protocols. *Lecture Notes in Computer Science*, 740:246–259, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sakurai:1993:SCS

[SI93b] K. Sakurai and T. Itoh. Subliminal channels for signature transfer and their application to signature distribution schemes. *Lecture Notes in Computer Science*, 718:231–243, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/021630.html.

Sakurai:1994:SCT

[SI94] K. Sakurai and T. Itoh. Subliminal channels for transferring signatures: Yet another cryptographic primitive. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E77–A(1):31–38, ???? 1994. CODEN IFESEX. ISSN 0916-8508 (print), 1745-1337 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/032631.html.

Sidhu:1981:APG

[Sid81] Deepinder P. Sidhu. Authentication protocols for general communication channels. In IEEE [IEE81], pages 30–40. CODEN CLCPDN. LCCN TK 5105.5 C66 1981. IEEE catalog no. 81CH1690-7.

Sieminski:1983:SBB

[Sie83] Gregory C. Sieminski. The search for a balance between scientific freedom and national security: a case study of cryptology. Thesis (M.S.), Defense Intelligence College, Washington, DC, USA, November 1983. v + 73 pp.

Siegenthaler:1984:CIN

[Sie84] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Siegenthaler:1985:DCS

[Sie85] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on Computers*, C34:81–85, 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). This paper breaks the cipher of [Gef73].

Swartzlander:1993:SCA

[SIJ93] Earl Swartzlander, Jr., Mary Jane Irwin, and Graham Jullien, editors. *Proceedings: 11th Symposium on Computer Arithmetic, June 29–July 2, 1993, Windsor, Ontario*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1993. ISBN 0-7803-1401-8 (softbound), 0-8186-3862-1 (casebound), 0-8186-3861-3 (microfiche). ISSN 0018-9340 (print), 1557-9956 (electronic). LCCN QA 76.9 C62 S95 1993. IEEE Transactions on Computers **43(8)**, 1994.

Shimbo:1993:CSC

[SiK93] Atsushi Shimbo and Shin ichi Kawamura. Cryptanalysis of several conference key distribution schemes. *Lecture Notes in Computer Science*, 739:265–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Silverman:1983:RVS

[Sil83] Jonathan M. Silverman. Reflections on the verification of the security of an operating system kernel. *Operating Systems Review*, 17 (5):143–154, October 1983. CODEN OSRED8. ISSN 0163-5980.

Silverman:1987:MPQ

[Sil87] Robert D. Silverman. The multiple polynomial quadratic sieve. *Mathematics of Computation*, 48(177):329–339, January 1987. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Silverman:1997:RSP

[Sil97a] R. D. Silverman. The requirement for strong primes in RSA. Technical note, RSA Data Security, Inc., Redwood City, CA, USA, May 17, 1997. URL `http://www.rsa.com/rsalabs/html/tech_notes.html`.

Silverman:1997:FGR

[Sil97b] Robert D. Silverman. Fast generation of random, strong RSA primes. *CryptoBytes*, 3(1):9–13, Spring 1997. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto3n1.pdf`.

Silverman:1999:EMM

[Sil99] Robert D. Silverman. Exposing the mythical MIPS year. *Computer*, 32(8):

22–26, August 1999. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co1999/pdf/r8022.pdf; http://www.computer.org/computer/co1999/r8022abs.htm.

Simonetta:1404:LTC

[Sim04] Cicco Simonetta. *[Little tract on cryptanalysis]*. ????, ????, 1404. ???? pp.

Simmons:1979:HID

[Sim79a] G. J. Simmons. How to insure that data acquired to verify treaty compliance are trustworthy. In IEEE, editor, *IEEE EASCON '79, Washington, DC, 1979*, pages 661–662. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1979. ISBN ???? LCCN ????

Simmons:1979:CCA

[Sim79b] Gustavus J. Simmons. Computational complexity and asymmetric encryption. In *Proceedings of the Eighth Manitoba Conference on Numerical Mathematics and Computing (Univ. Manitoba, Winnipeg, Man., 1978)*, Congress. Numer., XXII, pages 65–93. Utilitas Mathematica Publishers, Winnipeg, Manitoba, Canada, 1979.

Simmons:1979:SAE

[Sim79c] Gustavus J. Simmons. Symmetric and asymmetric encryption. *ACM Computing Surveys*, 11(4):305–330, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Simmons:1982:SCA

[Sim82a] Gustavus J. Simmons, editor. *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Selected Symposia Series*. Westview Press, Boulder, CO, 1982. ISBN 0-86531-338-5. x + 338 pp.

Simmons:1982:SAE

[Sim82b] Gustavus J. Simmons. Symmetric and asymmetric encryption. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 241–298. Westview Press, Boulder, CO, USA, 1982.

Simmons:1983:PPS

[Sim83] G. J. Simmons. The prisoners' problem and the subliminal channel. In Chaum et al. [CRS83], pages 51–67. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1001.html.

Simmons:1984:HID

[Sim84] G. J. Simmons. How to insure that data acquired to verify treaty compliance are trustworthy. *Proceedings of the IEEE*, 76(5):621–627, May 1984. CODEN IEEPAD. ISSN 0018-9219. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1003.html.

Simmons:1985:ATC

[Sim85a] Gustavus J. Simmons. Authentication theory/coding theory. In Blakley and Chaum [BC85], pages 411–431. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=411. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Simmons:1985:SCD

[Sim85b] Gustavus J. Simmons. The subliminal channel and digital signatures. In Beth et al. [BCI85], pages 364–378. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1002.html. Held at the University of Paris, Sorbonne.

Simmons:1988:SSC

[Sim88] G. J. Simmons. *Special section on cryptology*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. 533–627 pp.

Simmons:1990:HRS

[Sim90a] G. J. Simmons. How to (really) share a secret. In Goldwasser [Gol90b], pages 390–449. CODEN LNCSD9. ISBN 0-387-97196-3 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1988. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0403.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=403.

Simmons:1990:PSS

[Sim90b] Gustavus J. Simmons. Prepositioned shared secret and/or shared control schemes (invited). *Lecture Notes in Computer Science*, 434:436–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340436.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340436.pdf`.

Simmons:1991:GSS

[Sim91] Gustavus J. Simmons. Geometric shared secret and/ or shared control schemes (invited talk). *Lecture Notes in Computer Science*, 537:216–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370216.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370216.pdf`.

Simmons:1992:CCS

[Sim92] Gustavus J. Simmons, editor. *Contemporary Cryptology: the science of information integrity*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-87942-277-7. xv + 640 pp. LCCN QA76.9.A25 C6678 1992. US$79.95. IEEE order number: PC0271-7.

Simmons:1993:SCU

[Sim93] G. J. Simmons. The subliminal channels in the US Digital Signature Algorithm (DSA). In Wolfowicz [Wol93b], pages 35–54. LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/022612.html`.

Simmons:1994:CTS

[Sim94a] Gustavus J. Simmons. The consequences of trust in shared secret schemes. *Lecture Notes in Computer Science*, 765:448–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650448.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650448.pdf`.

Simmons:1994:CPF

[Sim94b] Gustavus J. Simmons. Cryptanalysis and protocol failures. *Communications of the Association for Computing Machinery*, 37(11): 56–65, November 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/188298.html`.

Simmons:1994:SCP

[Sim94c] Gustavus J. Simmons. Subliminal channels; past and present. *European transactions on telecommunications and related technologies*, 5(4):459–473, July–August 1994. CODEN ETTTET. ISSN 1120-3862. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/034412.html.

Simmons:1994:SCE

[Sim94d] Gustavus J. Simmons. Subliminal communication is easy using the DSA. In Helleseth [Hel94], pages T65–T81. CODEN LNCSD9. ISBN 3-540-57600-2 (Berlin), 0-387-57600-2 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1993. DM86.00. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/023619.html.

Simovits:1995:EDE

[Sim95] Mikael J. Simovits. *The DES, an extensive documentation and evaluation of the Data Encryption Standard*. Number 68 in A cryptographic series. Aegean Park Press, Laguna Hills, CA, USA, 1995. ISBN 0-89412-248-7. 116 pp. LCCN QA76.9.A25S553 1995.

Simmons:1996:HSC

[Sim96a] Gustavus J. Simmons. The history of subliminal channels. In Anderson [And96c], pages 237–256. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054161.html.

Simpson:1996:RPC

[Sim96b] W. Simpson. RFC 1994: PPP challenge handshake authentication protocol (CHAP), August 1996. URL ftp://ftp.internic.net/rfc/rfc1334.txt; ftp://ftp.internic.net/rfc/rfc1994.txt; https://www.math.utah.edu/pub/rfc/rfc1334.txt; https://www.math.utah.edu/pub/rfc/rfc1994.txt. Obsoletes RFC1334 [LS92]. Status: DRAFT STANDARD.

Simmons:1997:SCS

[Sim97] G. J. Simmons. Subliminal channels: Some recent developments. In Anonymous [Ano97a], page ?? LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061457.html.

Simmons:1998:HSC

[Sim98a] G. J. Simmons. The history of subliminal channels. *IEEE Journal on Selected Areas in Communications*, 16(4):452–462, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072153.html.

Simmons:1998:RCB

[Sim98b] G. J. Simmons. Results concerning the bandwidth of subliminal channels. *IEEE Journal on Selected Areas in Communications*, 16(4): 463–473, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072441.html.

Simon:1998:FCO

[Sim98c] Daniel R. Simon. Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? *Lecture Notes in Computer Science*, 1403:334–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030334.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030334.pdf.

Sinkov:1966:ECM

[Sin66] Abraham Sinkov. *Elementary cryptanalysis: a mathematical approach*, volume 22 of *New mathematical library*. Mathematical Association of America, Washington, DC, USA, 1966. ISBN 0-88385-622-0. ix + 222 pp. LCCN Z 104 S47 1980. With a supplement by Paul L. Irwin. Reissued in 1975 and 1980.

Sinkov:1968:ECMa

[Sin68a] Abraham Sinkov. *Elementary cryptanalysis: a mathematical approach*, volume 22 of *New mathematical library*. Random House, New York, NY, USA, 1968. ix + 189 pp. LCCN QA11 .N5 v.22.

Sinkov:1968:ECMb

[Sin68b] Abraham Sinkov. *Elementary cryptanalysis: a mathematical approach*, volume 22 of *New mathematical library*. Mathematical Association of America, Washington, DC, USA, 1968. ix + 222 pp.

Sinnott:1977:CTC

[Sin77] Robert Sinnott. *A catalogue of titles on chess, checkers, and cryptology in the library of the United States Military Academy, West Point, New York*. ????, Norwell, MA, USA, 1977. 35 pp.

Singh:1985:IPS

[Sin85] Kamaljit Singh. On improvements to password security. *Operating Systems Review*, 19(1):53–60, January 1985. CODEN OSRED8. ISSN 0163-5980.

Sinha:1995:KNC

[Sin95] Bappaditya Sinha. Kerberos for non-secure client-server applications. Thesis (M.S.), Arizona State University, Tempe, AZ, USA, 1995. vii + 49 pp.

Singer:1998:ECD

[Sin98] Anthony Martin Singer. Electronic commerce: digital signatures and the role of the Kansas Digital Signature Act. *Washburn law journal*, 37(3):725–745, Spring 1998.

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].

Siu:1999:PNG

[Siu99] Chi Sang Obadiah Siu. Pseudorandom number generator by cellular automata and its application to cryptography. M.Phil., Chinese University of Hong Kong, Hong Kong, 1999. 68 pp.

Sambur:1976:SEM

[SJ76] M. R. Sambur and N. S. Jayant. Speech encryption by manipulations of LPC parameters. *The Bell System Technical Journal*, 55(9):1373–1388, November 1976. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol55/bstj55-9-1373.pdf`.

Sethi:1997:FCS

[SJ97] Ishwar K. Sethi and Ramesh C. Jain, editors. *Fifth Conference on Storage and Retrieval for Image and Video Database, 13–14 February 1997, San Jose, CA, USA*, volume 3022 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 1997. ISBN 0-8194-2433-1. LCCN TS510.S63 v.3022.

Scott:1998:DAB

[SJS98] A. Scott, K. Jenkin, and R. Senjen. Design of an agent-based, multi-user scheduling implementation. *Lecture Notes in Computer Science*, 1544: 152–165, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sako:1994:SVU

[SK94] Kazue Sako and Joe Kilian. Secure voting using partially compatible homomorphisms. In Desmedt [Des94b], pages 411–424. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390411.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0839/08390411.pdf`.

Sako:1995:RFM

[SK95] K. Sako and J. Kilian. Receipt-free mix-type voting schemes. In Guillou and Quisquater [GQ95], pages 393–403. CODEN LNCSD9. ISBN 3-540-59409-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C794 1995. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1025.html`.

Schneier:1996:AOC

[SK96a] B. Schneier and J. Kelsey. Authenticating outputs of computer software using a cryptographic coprocessor. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1996. 14 pp. URL `http://www.counterpane.com/authenticating_outputs.html`. Also published in *Proceedings 1996 CARDIS, September 1996*, pp. 11–24.

Schneier:1996:PPSa

[SK96b] B. Schneier and J. Kelsey. A peer-to-peer software metering system. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, November 1996. URL `http://www.counterpane.com/meter-pp.html`. Also published in *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 279–286.

Schneier:1996:UFNa

[SK96c] B. Schneier and J. Kelsey. Unbalanced Feistel networks and block cipher design. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, February 1996. URL `http://www.counterpane.com/unbalanced_feistel.html`. Also published in *Fast Software Encryption, Third International Workshop Proceedings (February 1996)*, Springer-Verlag, 1996, pp. 121–144.

Schneier:1996:UFNb

[SK96d] B. Schneier and J. Kelsey. Unbalanced Feistel networks and block cipher design. *Lecture Notes in*

Computer Science, 1039: 121–144, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.counterpane.com/unbalanced_feistel.html.

Schneier:1996:PPSb

[SK96e] Bruce Schneier and John Kelsey. A peer-to-peer software metering system. In USENIX [USE96d], pages 279–286. ISBN 1-880446-83-9. LCCN HF5004 .U74 1996. URL http://www.usenix.org/publications/library/proceedings/ec96/index.html.

Schneier:1997:AESb

[SK97a] B. Schneier and J. Kelsey. Automatic event-stream notarization using digital signature. *Lecture Notes in Computer Science*, 1189: 155–169, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schneier:1997:AESa

[SK97b] B. Schneier and J. Kelsey. Automatic event-stream notarization using digital signatures. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1997. URL http://www.counterpane.com/event_stream.html. Also published in *Security Protocols, International Workshop April 1996 Proceedings*, Springer-Verlag, 1997, pp. 155–169 [SK97a].

Schneier:1997:RAS

[SK97c] B. Schneier and J. Kelsey. Remote auditing of software outputs using a trusted coprocessor. *Future Generation Computer Systems*, 13 (1):9–18, 1997. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.counterpane.com/remote_auditing.html.

Stabell-Kulo:1997:SLS

[SK97d] Tage Stabell-Kulø. Security and log structured file systems. *Operating Systems Review*, 31(2):9–10, April 1997. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Schneier:1998:CSS

[SK98a] B. Schneier and J. Kelsey. Cryptographic support for secure logs on untrusted machines. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, January 1998. 10 pp. URL http://www.counterpane.com/secure-logs.html. Also published in The Seventh USENIX Security Symposium Proceedings, USENIX Press, January 1998, pp. 53–62.

Shimoyama:1998:QRS

[SK98b] T. Shimoyama and T. Kaneko. Quadratic relation of S-box and its application to the linear attack of full round DES. *Lecture Notes in Computer Science*, 1462: 200–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shimoyama:1998:QRB

[SK98c] Takeshi Shimoyama and Toshinobu Kaneko. Quadratic relation of S-box and its application to the linear attack of full round DES. *Lecture Notes in Computer Science*, 1462: 200–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620200.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620200.pdf`.

Schneier:1999:SAL

[SK99] Bruce Schneier and John Kelsey. Secure audit logs to support computer forensics. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1999. URL `http://www.counterpane.com/audit-logs.html`. ACM Transactions on Information and System Security, v. 1, n. 3, 1999, to appear.

Stabell-Kulo:1999:PAM

[SKAM99] Tage Stabell-Kulø, Ronny Arild, and Per Harald Myrvang. Providing authentication to messages signed with a Smart Card in hostile environments. In USENIX [USE99c], page ?? ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL `http://www.usenix.org/publications/library/proceedings/smartcard99/stabell.html`.

Shepherd:1997:EKE

[SKB97] S. J. Shepherd, A. H. Kemp, and S. K. Barton. An efficient key exchange protocol for cryptographically secure CDMA systems. In ????, editor, *PIMRC '97, 1-4 September 1997, Helsinki*, page ?? ????, ????, 1997. ISBN ???? LCCN ????

Schell:19xx:CMC

[SKBxx] R. R. Schell, K. W. Kingdon, and T. A. Berson. Controlled modular cryptography apparatus and method. U.S. Patent 5,933,503., 19xx.

Sorokine:1994:TBD

[SKD94] V. Sorokine, F. R. Kschischang, and V. Durand.

Trellis-based decoding of binary linear block codes. *Lecture Notes in Computer Science*, 793:270–286, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Suzuki:1999:AVB

[SKIT99] S. Suzuki, T. Kato, H. Ishizuka, and Y. Takahashi. An application of vision-based learning in RoboCup for a real robot with an omnidirectional vision system and the team description of Osaka University "Trackies". *Lecture Notes in Computer Science*, 1604:316–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Satoh:1998:HSR

[SKNO98a] A. Satoh, Y. Kobayashi, H. Niijima, and N. Ooba. A high-speed small RSA encryption LSI with low power dissipation. *Lecture Notes in Computer Science*, 1396:174–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Satoh:1998:HSS

[SKNO98b] A. Satoh, Y. Kobayashi, H. Niijima, and N. Ooba. A high-speed small RSA encryption LSI with low power dissipation. *Lecture Notes in Computer Science*, 1396:174–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schneier:1996:DP

[SKW96] B. Schneier, J. Kelsey, and J. Walker. Distributed proctoring. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, September 1996. URL `http://www.counterpane.com/distributed_proctoring.html`. Also published in *ESORICS 96 Proceedings*, Springer-Verlag, September 1996, pp. 172–182.

Schneier:1998:TKSa

[SKW+98a] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. On the Twofish key schedule. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1998. URL `http://www.counterpane.com/twofish-keysched.html`. To appear in *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998.

Schneier:1998:TBBa

[SKW+98b] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. Twofish: a 128-bit block cipher. Technical report, Counterpane Systems, 101

East Minnehaha Parkway, Minneapolis, MN 55419, June 15, 1998. URL http://www.counterpane.com/twofish-paper.html.

Schneier:1998:TBBb

[SKW+98c] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. Twofish: a 128-bit block cipher. Evaluation CD-1: Documentation, National Institute of Standards and Technology, August 1998.

Schneier:1998:TSC

[SKW+98d] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. Twofish on smart cards. In ????, editor, *Proceedings of CARDIS 98*, page ?? Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN ???? LCCN ????

Schneier:1998:TBE

[SKW+98e] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. Twofish: a block encryption algorithm. In National Institute of Standards and Technology [Nat98], page 16. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf1/twofish-slides.pdf. See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen "complete and proper" candidates.

Schneier:1998:TNB

[SKW+98f] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. Twofish: a new block cipher. In National Institute of Standards and Technology [Nat98], page ?? ISBN ???? LCCN ???? URL http://www.counterpane.com/twofish.html. No slides for the conference talk are available.

Schneier:1999:PCAa

[SKW+99a] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. Performance comparison of the AES submissions. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, April 1999. 19 pp. URL http://www.counterpane.com/aes-performance.html. Second AES Candidate Conference, April 1999, to appear.

Schneier:1999:PCAb

[SKW+99b] B. Schneier, J. Kelsey, D. Whiting, D. Wagner,

C. Hall, and N. Ferguson. Performance comparison of the AES submissions. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf2/Schneier.pdf`. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen "complete and proper" candidates.

Schneier:1999:APC

[SKW+99c] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. AES performance comparisons. In National Institute of Standards and Technology [Nat99b], page 44. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf2/Schneier.pdf; http://www.counterpane.com/twofish`. Only the slides for the conference talk are available, but technical reports are available at the authors' Web site.

Schneier:1999:NRT

[SKW+99d] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. New results on the Twofish encryption algorithm. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, April 1999. 13 pp. URL `http://www.counterpane.com/twofish-aes.html`. Second AES Candidate Conference, April 1999, to appear.

Schneier:1999:TEAb

[SKW+99e] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. *The Twofish Encryption Algorithm*. John Wiley and Sons, Inc., New York, NY, USA, 1999. ISBN 0-471-35381-7. xi + 186 pp. LCCN QA76.9.A25 T85 1999. US$50. URL `http://www.counterpane.com/twofish-book.html`.

Schneier:1996:AC

[SKWH96] B. Schneier, J. Kelsey, D. Wagner, and C. Hall. An authenticated camera. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, December 1996. URL `http://www.counterpane.com/camera.html`. Also published in *12th Annual Computer Security Applications Conference*, ACM Press, December 1996, pp. 24–30.

Schneier:1999:TKS

[SKWW99] B. Schneier, J. Kelsey, D. Whiting, and D. Wagner.

On the Twofish key schedule. *Lecture Notes in Computer Science*, 1556:27–42, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sufatrio:1999:IMS

[SL99] Sufatrio and Kwok-Yan Lam. Internet mobility support optimized for client access and its scalable authentication framework. *Lecture Notes in Computer Science*, 1748:220–229, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1748/17480220.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1748/17480220.pdf`.

Slutsky:1998:KDQ

[Slu98] Boris Slutsky. *Key distillation in quantum cryptography*. Thesis (Ph. D.), Department of Electrical Engineering, University of California, San Diego, San Diego, CA, USA, 1998. xiii + 155 pp.

Schobi:1983:FAT

[SM83] P. Schöbi and J. L. Massey. Fast authentication in a trapdoor-knapsack public key cryptosystem. *Lecture Notes in Computer Science*, 149:289–306, 1983. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Siromoney:1990:PKC

[SM90] Rani Siromoney and Lisa Mathew. A public key cryptosystem based on Lyndon words. *Information Processing Letters*, 35(1):33–36, June 15, 1990. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Staffelbach:1991:CSC

[SM91] O. Staffelbach and W. Meier. Cryptographic significance of the carry for ciphers based on integer addition. *Lecture Notes in Computer Science*, 537:601–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schubert:1995:MLS

[SM95a] T. Schubert and S. Mocas. A mechanized logic for secure key escrow protocol verification. *Lecture Notes in Computer Science*, 971:308–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Syverson:1995:FRK

[SM95b] P. Syverson and C. Meadows. Formal requirements for key distribution protocols. *Lecture Notes in Computer Science*, 950:320–331,

1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sklower:1996:RPE

[SM96] K. Sklower and G. Meyer. RFC 1969: The PPP DES encryption protocol (DESE), June 1996. URL ftp://ftp.internic.net/rfc/rfc1969.txt; ftp://ftp.internic.net/rfc/rfc2419.txt; https://www.math.utah.edu/pub/rfc/rfc1969.txt; https://www.math.utah.edu/pub/rfc/rfc2419.txt. Obsoleted by RFC2419 [SM98b]. Status: INFORMATIONAL.

Schneier:1998:CMP

[SM98a] B. Schneier and Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP). Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, November 1998. 10 pp. URL http://www.counterpane.com/pptp-paper.html. *Proceedings of the 5th ACM Conference on Communications and Computer Security*, ACM Press, November 1998, to appear.

Sklower:1998:RPE

[SM98b] K. Sklower and G. Meyer. RFC 2419: The PPP DES encryption protocol, version 2 (DESE-bis), September 1998. URL ftp://ftp.internic.net/rfc/rfc1969.txt; ftp://ftp.internic.net/rfc/rfc2419.txt; https://www.math.utah.edu/pub/rfc/rfc1969.txt; https://www.math.utah.edu/pub/rfc/rfc2419.txt. Obsoletes RFC1969 [SM96]. Status: PROPOSED STANDARD.

Sutcliffe:1999:LBM

[SM99] A. G. Sutcliffe and S. Minocha. Linking business modelling to socio-technical system design. *Lecture Notes in Computer Science*, 1626: 73–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smart:1999:PHC

[Sma99] N. P. Smart. On the performance of hyperelliptic cryptosystems. *Lecture Notes in Computer Science*, 1592: 165–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schneier:1999:DDE

[SMD+99] Bruce Schneier, Carl H. Meyer, Dorothy Elizabeth Robling Denning, Douglas R. Stinson, A. J. Menezes, and William F. Friedman. *Dr. Dobb's essential books on cryptography and security.* Dr.

Dobb's CD-ROM library. Miller Freeman Publications, San Francisco, CA, USA, 1999. LCCN QA76.9.A25 D7 1999 Interactive Learning Center. Books on CD-ROM.

Smejkal:1997:DEI

[Sme97] Denise Smejkal. Data encryption and the Internet. Thesis (Honors), University of South Dakota, Vermillion, SD, USA, 1997. 10 pp.

Smith:1943:CSS

[Smi43] Laurence Dwight Smith. *Cryptography, the science of secret writing*. W. W. Norton & Co., New York, NY, USA, 1943. 164 pp. LCCN Z104 .S5.

Smith:1944:CSS

[Smi44] Laurence Dwight Smith. *Cryptography: the science of secret writing*. G. Allen and Unwin, London, UK, 1944. 164 pp. LCCN Z104.S5.

Smith:1955:CSS

[Smi55] Laurence Dwight Smith. *Cryptography; the science of secret writing*. Dover Publications, Inc., New York, NY, USA, 1955. 164 pp. LCCN Z104 .S6. "An unabridged republication of the first edition with corrections.".

Smith:1971:DLC

[Smi71a] J. L. Smith. The design of Lucifer, a cryptographic device for data communications. Research Report RC-3326, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, 1971.

Smith:1971:CSS

[Smi71b] Laurence Dwight Smith. *Cryptography, the science of secret writing*. Dover Publications, Inc., New York, NY, USA, 1971. ISBN 0-486-20247-X. 164 pp. LCCN Z 104 S65c 1971. "This Dover edition, first published in 1955, is an unabridged and corrected republication of the work originally published by W. W. Norton and Company in 1943." "Copyright renewed 1971." Bibliography: p. 156.

Smith:1974:RBC

[Smi74] J. L. Smith. Recirculating block cipher cryptographic system. U.S. Patent No. 3,796,830, March 12, 1974.

Smith:1983:PKC

[Smi83] John Smith. Public key cryptography: An introduction to a powerful cryptographic system for use on microcomputers. *BYTE Magazine*, 7(??):198–218, January 1983. CODEN BYTEDJ. ISSN 0360-5280.

This is a simple exposition of public key cryptography.

Smith:1987:AUW

[Smi87] Sidney L. Smith. Authenticating users by word association. *Computers and Security*, 6(6):464–470, December 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404887900277`.

Smith:1990:PPC

[Smi90] Jonathan M. Smith. Practical problems with a cryptographic protection scheme (invited). *Lecture Notes in Computer Science*, 435: 64–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350064.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350064.pdf`.

Smith:1993:ADA

[Smi93a] Douglas Smith. Automating the design of algorithms. *Lecture Notes in Computer Science*, 755:324–354, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smith:1993:LPE

[Smi93b] Peter Smith. LUC public-key encryption: a secure alternative to RSA. *Dr. Dobb's Journal of Software Tools*, 18(1):44, 46, 48–49, 90–92, January 1993. CODEN DDJOEB. ISSN 1044-789X.

Smith:1994:CPC

[Smi94a] Larry J. Smith. Cryptology, privacy and the Clipper chip. Thesis (M.S.), Texas Tech University, Lubbock, TX, USA, 1994. vi + 72 pp.

Smith:1994:CE

[Smi94b] Peter Smith. Cryptography without exponentiation. *Dr. Dobb's Journal of Software Tools*, 19(4):26, 28, 30, April 1994. CODEN DDJOEB. ISSN 1044-789X.

Smith:1997:ETC

[Smi97a] Marcia S. Smith. Encryption technology: Congressional issues. CRS issue brief IB96039, Congressional Research Service, The Library of Congress, Washington, DC, USA, January 2, 1997. 8 pp.

Smith:1997:IC

[Smi97b] Richard E. Smith. *Internet Cryptography*. Addison-Wesley, Reading, MA, USA, 1997. ISBN 0-201-92480-3. xx + 356 pp. LCCN TK5102.94.S65 1997. US$27.95.

Smith:1998:IES

[Smi98a] Mark T. Smith. Integrated engineering: Smart cards: Integrating for portable complexity. *Computer*, 31(8):110–112, August 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://dlib.computer.org/co/books/co1998/pdf/r8110.pdf`.

Smith:1998:SXC

[Smi98b] Michael Smith. *Station X: The Codebreakers of Bletchley Park*. Channel 4 Books, London, UK, 1998. ISBN 0-7522-7148-2. 184 pp. LCCN ???? UK£5.99.

Shimoyama:1998:IHO

[SMK98a] T. Shimoyama, S. Moriai, and T. Kaneko. Improving the higher order differential attack and cryptanalysis of the KN cipher. *Lecture Notes in Computer Science*, 1396:32–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Son:1998:ASC

[SMK98b] Jun Wan Son, Manabu Miyata, and Tomoaki Kawaguchi. Analyses of some cryptosystems based on the complexity of permutations. *Tensor (N.S.)*, 60 (2):213–218, 1998. CODEN TNSRAZ. ISSN 0040-3504.

Stakhov:1999:IFC

[SMS99] Alexei Stakhov, Vinancio Massingue, and Anna Sluchenkova. *Introduction into Fibonacci coding and cryptography*. Osnova, Kharkov State University, Kharkov, Russia, 1999. ISBN ???? ???? pp. LCCN ???? URL `http://www.goldenmuseum.com/1502EMU_engl.html`.

Safavi-Naini:1993:FTA

[SN93] Reihaneh Safavi-Naini. Feistel type authentication codes. *Lecture Notes in Computer Science*, 739: 170–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shepherd:1994:VFH

[SN94] S. J. Shepherd and J. M. Noras. A very fast hardware replacement for the DES. In ????, editor, *Proceedings of the Third UK/ Australian Symposium on DSP for Communications Systems, 12–14 December 1994, University of Warwick, UK*, page ?? ????, ????, 1994. ISBN ???? LCCN ????

Safavi-Naini:1996:TSS

[SN96] R. Safavi-Naini. Three systems for shared generation of authenticators. *Lecture Notes in Computer Science*, 1090:401–??, 1996. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smith:1972:EAC

[SNO72] J. L. Smith, W. A. Notz, and P. R. Osseck. An experimental application of cryptography to a remotely accessed data system. *Proceedings of the ACM 1972 Annual Conference*, ??(??): 282–297, ???? 1972.

Steiner:1988:KAS

[SNS88] Jennifer G. Steiner, Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An authentication service for open network systems. In USENIX Association [USE88c], pages 191–202. ISBN ???? LCCN ????

Safavi-Naini:1993:ACU

[SNT93] R. Safavi-Naini and L. Tombak. Authentication codes under impersonation attack. *Lecture Notes in Computer Science*, 718:35–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Safavi-Naini:1995:ACP

[SNT95] Reihaneh Safavi-Naini and L. Tombak. Authentication codes in plaintext and chosen-content attacks. *Lecture Notes in Computer Science*, 950: 254–265, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500254.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0950/09500254.pdf`.

Safavi-Naini:1998:BCM

[SNW98a] R. Safavi-Naini and H. Wang. Bounds and constructions for multireceiver authentication codes. *Lecture Notes in Computer Science*, 1514: 242–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Safavi-Naini:1998:NRM

[SNW98b] Reihaneh Safavi-Naini and Huaxiong Wang. New results on multi-receiver authentication codes. *Lecture Notes in Computer Science*, 1403:527–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1403/14030527.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1403/14030527.pdf`.

Snyder:1979:IUC

[Sny79] Samuel S. Snyder. Influence of U.S. Cryptologic Organizations on the digital computer industry. *The Journal of Systems and Software*, 1 (1):87–102, ???? 1979. CODEN JSSODM. ISSN 0164-1212.

Snyder:1980:CAP

[Sny80] Samuel S. Snyder. Computer advances pioneered by cryptologic organizations. *Annals of the History of Computing*, 2(1):60–70, January/March 1980. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1980/pdf/a1060.pdf; http://www.computer.org/annals/an1980/a1060abs.htm`.

Shepherd:1998:ALP

[SOB98] S. J. Shepherd, J. Orriss, and S. K. Barton. Asymptotic limits in peak envelope power reduction by redundant coding in QPSK multi-carrier modulation. *IEEE Transactions on Communications*, 46(1):5–10, January 1998. CODEN IECMBT. ISSN 0090-6778 (print), 1558-0857 (electronic).

Sonnino:1999:CBL

[Son99] Angelo Sonnino. Cryptosystems based on Latin rectangles and generalized affine spaces. *Rad. Mat.*, 9(2): 177–186 (2000), 1999. ISSN 0352-6100.

Schroeppel:1995:FKE

[SOOS95] R. Schroeppel, H. Orman, S. O'Malley, and O. Spatscheck. Fast key exchange with elliptic curve systems. *Lecture Notes in Computer Science*, 963: 43–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sorkis:1980:USM

[Sor80] Michael Sorkis. Use of statistically matched codes in a data encryption system. Thesis (M.S.), Southern Illinois University at Carbondale, Carbondale, IL, USA, 1980. v + 91 pp.

Soto:1998:RTA

[Sot98] Juan Soto, Jr. Randomness testing of the AES candidate algorithms. In National Institute of Standards and Technology [Nat98], page 9. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/r1-rand.pdf`. See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen "complete and proper" candidates.

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.

Seberry:1989:CIC

[SP89] Jennifer Seberry and Josef Pieprzyk. *Cryptography: an introduction to computer security*. Prentice Hall advances in computer science series. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, 1989. ISBN 0-13-194986-1. viii + 375 pp. LCCN QA76.9.A25 S371 1989.

Seberry:1990:ACA

[SP90] Jennifer Seberry and Josef Pieprzyk, editors. *Advances in cryptology — AUSCRYPT '90: international conference on cryptology, Sydney, Australia, January 8–11, 1990: proceedings*, volume 453 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. CODEN LNCSD9. ISBN 3-540-53000-2 (Berlin), 0-387-53000-2 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 A87 1990. DM63.00. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0453.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=453. Sponsored by the International Association for Cryptologic Research.

Spender:1987:ICU

[Spe87] J-C. Spender. Identifying computer users with authentication devices (tokens). *Computers and Security*, 6(5):385–395, October 1987. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404887900113.

Schechter:1999:AAM

[SPH99] Stuart Schechter, Todd Parnell, and Alexander Hartemink. Anonymous authentication of membership in dynamic groups. In Franklin [Fra99], pages 184–195. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999. URL http://link.springer-ny.com/link/service/series/0558/bibs/1648/16480184.htm; http://link.springer-ny.com/link/service/series/0558/papers/1648/16480184.pdf.

Spirakis:1995:AET

[Spi95] P. G. Spirakis, editor. *Algorithms — ESA '95: Third Annual European Symposium, Corfu, Greece, September 25–27, 1995: proceedings*, volume 979 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-60313-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A43 E83 1995.

Schwemmlein:1998:RMR

[SPP98] J. Schwemmlein, K. C. Posch, and R. Posch. RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography. *Computers and Security*, 17(7):637–650, ???? 1998. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404899800613.

Schuett:1997:CPB

[SPS97] D. Schuett, F. Pichler, and J. Scharinger. Cryptographic permutations based on BOOT decompositions of Walsh matrices. *Lecture Notes in Computer Science*, 1333:580–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shoup:1996:SKD

[SR96] Victor Shoup and Avi Rubin. Session key distribution using smart cards. *Lecture Notes in Computer Science*, 1070:321–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700321.htm; http://link.springer-ny.com/link/service/series/0558/papers/1070/10700321.pdf.

Saltzer:1984:EEA

[SRC84] J. H. Saltzer, D. P. Reed, and D. D. Clark. End-to-end arguments in system design. *ACM Transactions on Computer Systems*, 2(4):277–288, November 1984. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Shin:1998:NHF

[SRRL98] Sang Uk Shin, Kyung Hyune Rhee, Dae Hyun Ryu, and Sang Jin Lee. A new hash function based on MDx-family and its application to MAC. *Lecture Notes in Computer Science*, 1431:234–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shin:1999:HFM

[SRY99] Sang Uk Shin, Kyung Hyune Rhee, and Jae Woo Yoon. Hash functions and the MAC using all-or-nothing property. *Lecture Notes in Computer Science*, 1560: 263–275, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shamir:1984:CCV

[SS84] A. Shamir and C. P. Schnorr. Cryptanalysis of certain variants of Rabin's signature scheme. *Information Processing Letters*, 19(3):113–115, October 19, 1984. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Siromoney:1986:PKC

[SS86] Rani Siromoney and Gift Siromoney. A public key cryptosystem that defies cryptanalysis. In *Workshop on Mathematics of Computer Algorithms (Madras, 1986)*, volume 111 of *IMS Rep.*, pages D.3.17, 4. Inst. Math. Sci., Madras, 1986.

Shepherd:1989:CSS

[SS89] S. J. Shepherd and P. W. Sanders. A comprehensive security service - functional specification. Ibm internal document, IBM (United Kingdom Laboratories), Hursley Park, Winchester, UK, May 1989.

Shepherd:1990:DSA

[SS90] S. J. Shepherd and P. W. Sanders. A distributed security architecture for large scale systems. In ????, editor, *Proceedings of the International Federation of Information Processing (IFIP) International Workshop on Distributed Systems Operations and Management, Berlin, 22–23 October 1990*, page ?? ????, ????, 1990. ISBN ???? LCCN ????

Schrift:1991:UNB

[SS91] A. W. Schrift and Adi Shamir. On the universality of the next bit test. *Lecture Notes in Computer Science*, 537:394–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370394.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370394.pdf`.

Sun:1994:DTS

[SS94] Hung Min Sun and Shiuh Pyng Shieh. On dynamic threshold schemes. *Information Processing Letters*, 52 (4):201–206, November 25, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sakurai:1995:RAC

[SS95a] K. Sakurai and H. Shizuya. Relationships among the computational powers of breaking discrete log cryptosystems. *Lecture Notes in Computer Science*, 921: 341–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smith:1995:PCD

[SS95b] P. Smith and C. Skinner. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms. *Lecture Notes in Computer Science*, 917:357–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smith:1995:PKC

[SS95c] P. Smith and C. Skinner. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms. *Lecture Notes in Computer Science*, 917:357–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sandhu:1996:AAC

[SS96] Ravi Sandhu and Pierangela Samarati. Authentication, access control, and audit. *ACM Computing Surveys*, 28(1):241–243, March 1996. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `http://www.acm.org/pubs/citations/journals/surveys/1996-28-1/p241-sandhu/`; `http://www.acm.org/pubs/toc/Abstracts/surveys/234412.html`.

Silverman:1997:CAX

[SS97] B. Silverman and J. Stapleton. Contribution to ANSI X9F1. Unpublished communication., December 1997.

Sakai:1998:DHC

[SS98a] Yasuyuki Sakai and Kouichi Sakurai. Design of hyperelliptic cryptosystems in small characteristic and a software implementation over F_{2^n}. *Lecture Notes in Computer Science*, 1514: 80–94, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sun:1998:PKC

[SS98b] Hung-Min Sun and Shiuh-Pyng Shieh. On private-key cryptosystems based on product codes. *Lecture Notes in Computer Science*, 1438:68–79, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schneier:1999:BHD

[SS99a] B. Schneier and A. Shostack. Breaking up is hard to do: Modeling security threats for smart cards. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1999. URL http://www.counterpane.com/smart-card-threats.html. *First USENIX Symposium on Smart Cards*, USENIX Press, to appear.

Schoenhoff:1999:GVM

[SS99b] M. Schoenhoff and M. Straessler. Global version management for a federated turbine design environment. *Lecture Notes in Computer Science*, 1649:203–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shapiro:1999:MAE

[SS99c] Jim Shapiro and David Shapiro. MMPC: An algorithm for encrypting multiple messages. *Dr. Dobb's Journal of Software Tools*, 24(12):32, 34, 36, 38, 40–41, December 1999. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ftp/1999/1999_12/mmpc.txt; http://www.ddj.com/ftp/1999/1999_12/mmpc.zip.

Solomonides:1999:REI

[SS99d] C. Solomonides and M. Searle. Relevance of existing intelligent network infrastructure to the Internet. *Lecture Notes in Computer Science*, 1597:459–468, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stubblebine:1999:FLA

[SS99e] S. G. Stubblebine and P. F. Syverson. Fair on-line auctions without special trusted parties. *Lecture Notes in Computer Science*, 1648:230–240, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stubblebine:1999:FOA

[SS99f] S. G. Stubblebine and P. F. Syverson. Fair on-line auctions without special trusted parties. In Franklin [Fra99], pages 230–240. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Subramanian:1987:DTP

[SSA87] K. G. Subramanian, Rani Siromoney, and P. Jeyanthi Abisha. A D0L-T0L public key cryptosystem. *Information Processing Letters*, 26(2):95–97, October 19, 1987. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Siromoney:1988:CPL

[SSA88] R. Siromoney, K. G. Subramanian, and Jeyanthi Abisha. Cryptosystems for picture languages. In *Syntactic and structural pattern recognition (Barcelona and Sitges, 1986)*, volume 45 of *NATO Adv. Sci. Inst. Ser. F Comput. Systems Sci.*, pages 315–332. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988.

Saito:1999:DPC

[SSCP99] H. Saito, N. Stavrakos, S. Carroll, and C. Polychronopoulos. The design of the PROMIS compiler. *Lecture Notes in Computer Science*, 1575:214–228, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smith:1981:VEP

[SSDG81] Michael K. Smith, Ann E. Siebert, Benedetto L. DiVito, and Donald I. Good. A verified encrypted packet interface. *ACM SIGSOFT Software Engineering Notes*, 6(3):13–16, July 1981. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Stubblebine:1999:UST

[SSG99] Stuart G. Stubblebine, Paul F. Syverson, and David M. Goldschlag. Unlinkable serial transactions: protocols and applications. *ACM Transactions on Information and System Security*, 2(4):354–389, November 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org/pubs/articles/journals/tissec/1999-2-4/p354-stubblebine/p354-stubblebine.pdf; http://www.acm.org/pubs/citations/journals/tissec/1999-2-4/p354-stubblebine/.

Safford:1993:SRA

[SSH93] David R. Safford, Douglas Lee Schales, and David K. Hess. Secure RPC authentication (SRA) for TELNET and FTP. In USENIX Association [USE93], pages 63–67. ISBN 1-880446-55-3. LCCN QA 76.9 A25 U54 1993. URL http://www.usenix.org/publications/library/proceedings/sec4/rpc.saf.html.

Sakai:1997:WRK

[SSI97a] Y. Sakai, K. Sakurai, and I. Ishizuka. On weak RSA-keys produced from Pretty Good Privacy. *Lecture Notes in Computer Science*, 1334:314–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sakai:1997:WRP

[SSI97b] Y. Sakai, K. Sakurai, and I. Ishizuka. On weak RSA-keys produced from Pretty Good Privacy. *Lecture Notes in Computer Science*, 1334:314–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sakai:1998:SHC

[SSI98] Y. Sakai, K. Sakurai, and H. Ishizuka. Secure hyperelliptic cryptosystems and their performance. *Lecture Notes in Computer Science*, 1431:164–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Subramanian:1992:LT

[SSM92] K. G. Subramanian, R. Siromoney, and L. Mathew. Lyndon trees. *Theoretical Computer Science*, 106 (2):373–383, December 14, 1992. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Sherman:1994:SNA

[SSM94] S. A. Sherman, R. Skibo, and R. S. Murray. Secure network access using multiple applications of AT&T's Smart Card. *AT&T Technical Journal*, 73(5):61–72, September/October 1994. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).

Schneier:1997:DDE

[SSM+97] Bruce Schneier, D. R. Stinson, A. J. Menezes, Dorothy Elizabeth Robling Denning, Carl H. Meyer, and William F. Friedman. *Dr. Dobb's essential books on cryptography and security*. Dr. Dobb's CD-ROM library 14. Miller Freeman Publications, San Francisco, CA, USA, 1997. Include one CD-ROM.

Saeednia:1998:NIK

[SSN98a] S. Saeednia and R. Safavi-Naini. A new identity-based key exchange protocol minimizing computation and communication. *Lecture Notes in Computer Science*, 1396:328–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Saeednia:1998:SGI

[SSN98b] S. Saeednia and R. Safavi-Naini. On the security of Girault's identification scheme. *Lecture Notes in Computer Science*, 1431: 149–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Susilo:1999:FST

[SSNP99] W. Susilo, R. Safavi-Naini, and J. Pieprzyk. Fail-stop threshold signature schemes based on elliptic curves. *Lecture Notes in*

Computer Science, 1587: 103–116, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shepherd:1990:CSS

[SSP90] S. J. Shepherd, P. W. Sanders, and A. Patel. A comprehensive security system — the concepts, agents and protocols. *Computers and Security*, 9(7):631–643, November 1990. CODEN CPSEDU. ISSN 0167-4048.

Schmidt:1998:LOA

[SSS98] B. Schmidt, M. Schimmler, and H. Schroeder. Long operand arithmetic on instruction systolic computer architectures and its application in RSA cryptography. *Lecture Notes in Computer Science*, 1470:916–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Salter:1998:TSS

[SSSW98] C. Salter, O. Saydjari, B. Schneier, and J. Wallner. Toward a secure system engineering methodology. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, September 1998. URL `http://www.counterpane.com/secure-methodology.html`. New Security Paradigms Workshop, September 1998, to appear.

Schneier:1998:DDE

[SSv+98] Bruce Schneier, Douglas Stinson, Paul van Oorschot, Scott Vanston, Alfred Menezes, Dorothy Denning, Carl Meyer, Stepehen Matyas, Richard Demillo, Gustavus Simmons, William Friedman, U.S.Army, and RSA Data Security. *Dr. Dobb's Essential Books on Cryptography and Security*. Dr. Dobb's CD-ROM Library, 1601 West 23rd, Suite 200, Lawrence, KS 66046-2703, USA, 1998. US$99.95. URL `mailto:orders@mfi.com`. CD ROM includes the text of twelve books and one newsletter.

StJohns:1984:RAS

[St.84] M. St. Johns. RFC 912: Authentication service, September 1, 1984. URL `ftp://ftp.internic.net/rfc/rfc912.txt; ftp://ftp.internic.net/rfc/rfc931.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc912.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc931.txt; https://www.math.utah.edu/pub/tex/bib/cryptography.bib`. Obsoleted by RFC0931 [St.85]. Status: UNKNOWN.

StJohns:1985:RAS

[St.85] M. St. Johns. RFC 931: Authentication server, January 1, 1985. URL `ftp://ftp.internic.net/`

rfc/rfc912.txt; ftp://ftp.internic.net/rfc/rfc931.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc912.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc931.txt. Obsoleted RFC1413 [St.93]. Obsoletes RFC0912 [St.84]. Status: UNKNOWN.

Shawe-Taylor:1989:BRB

[ST89] John Shawe-Taylor. Book review: *Cryptography: an introduction to computer security*, by Jennifer Seberry and Josef Pieprzyk. Prentice-Hall International, Hemel Hempstead, United Kingdom, 1988, Price £17.95 (paperback), ISBN 0-7248-0274-6. *Science of Computer Programming*, 12(3):259–260, September 1989. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic). URL http://www.sciencedirect.com/science/article/pii/0167642389900063.

Stern:1991:CPK

[ST91] Jacques Stern and Philippe Toffin. Cryptanalysis of a public-key cryptosystem based on approximations by rational numbers. *Lecture Notes in Computer Science*, 473:313–317, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730313.htm; http://link.springer-ny.com/link/service/series/0558/papers/0473/04730313.pdf.

StJohns:1993:RIP

[St.93] M. St. Johns. RFC 1413: Identification protocol, January 1993. URL ftp://ftp.internic.net/rfc/rfc1413.txt; ftp://ftp.internic.net/rfc/rfc931.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc1413.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc931.txt; https://www.math.utah.edu/pub/tex/bib/cryptography.bib. Obsoletes RFC0931 [St.85]. Status: PROPOSED STANDARD.

Safavi-Naini:1994:OAS

[ST94] R. Safavi-Naini and L. Tombak. Optimal authentication systems. *Lecture Notes in Computer Science*, 765: 12–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650012.htm; http://link.springer-ny.com/link/service/series/0558/papers/0765/07650012.pdf.

Stark:1970:INT

[Sta70] Harold M. Stark. *An introduction to number the-*

ory. Markham mathematics series. Markham Publishing Company, Chicago, IL, USA, 1970. ISBN 0-8410-1014-5. x + 347 pp. LCCN QA241 .S72.

Stark:1978:INT

[Sta78] Harold M. Stark. *An introduction to number theory*. MIT Press, Cambridge, MA, USA, 1978. ISBN 0-262-69060-8. x + 347 pp. LCCN QA241 .S72 1978.

Stallings:1994:PGP

[Sta94a] William Stallings. Pretty Good Privacy: Privacy and security are important issues to commercial users of public E-mail systems. PGP, an E-mail security package, is finding acceptance as the way to achieve protection. *BYTE Magazine*, 19(7):193–??, July 1994. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Stallings:1994:SSH

[Sta94b] William Stallings. SHA: The Secure Hash Algorithm. *Dr. Dobb's Journal of Software Tools*, 19(4):32, 34, April 1, 1994. CODEN DDJOEB. ISSN 1044-789X.

Stallings:1995:PWT

[Sta95a] William Stallings. The PGP web of trust: Managing public keys with the PGP (Pretty Good Privacy) web of trust. *BYTE Magazine*, 20(2):161–??, February 1995. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Stallings:1995:PYP

[Sta95b] William Stallings. *Protect your privacy: the PGP user's guide*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 1995. ISBN 0-13-185596-4. xvi + 302 pp. LCCN TK5102.85.S73 1995. With a foreword by Phil Zimmermann.

Stadler:1996:PVS

[Sta96a] M. Stadler. Publicly verifiable secret sharing. *Lecture Notes in Computer Science*, 1070:190–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Staiger:1996:CSW

[Sta96b] Ludwig Staiger. Codes, simplifying words, and open set condition. *Information Processing Letters*, 58(6):297–301, June 24, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Stallings:1996:PCS

[Sta96c] William Stallings. Patching the cracks in SNMP. *BYTE Magazine*, 21(8):55–??, August 1996. CODEN BYTEDJ. ISSN 0360-5280

(print), 1082-7838 (electronic).

Stallings:1996:PCI

[Sta96d] William Stallings. *Practical cryptography for internetworks*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN 0-8186-7140-8 (paperback). x + 356 pp. LCCN TK5105.59 .S73 1996.

Staddon:1997:CSC

[Sta97a] Jessica Nicola Staddon. *A combinatorial study of communication, storage and traceablity in broadcast encryption systems*. Thesis (Ph. D. in Mathematics), Department of Mathematics, University of California, Berkeley, Berkeley, CA, USA, December 1997. v + 43 pp.

Stallman:1997:SDR

[Sta97b] Richard Stallman. Societal dimensions: The right to read. *Communications of the Association for Computing Machinery*, 40(2):85–87, February 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/citations/journals/cacm/1997-40-2/p85-stallman/`.

Stark:1997:ESP

[Sta97c] Thom Stark. Encryption for a small planet — U.S. restrictions on encryption exports are cramping development of secure international applications. what are your options for competing in the world market? *BYTE Magazine*, 22(3):111–??, March 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Stallings:1999:CNS

[Sta99a] William Stallings. *Cryptography and network security: principles and practice*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, second edition, 1999. ISBN 0-13-869017-0. xvii + 569 pp. LCCN TK5105.59.S713 1999. URL `http://www.prenhall.com/allbooks/esm_0138690170.html`.

Stallings:1999:HAK

[Sta99b] William Stallings. The HMAC algorithm: Key hashing for message authentication. *Dr. Dobb's Journal of Software Tools*, 24 (4):46, 48–49, April 1999. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ftp/1999/1999_04/hmac.txt`.

Stevenson:1976:MCI

[Ste76] William Stevenson. *A man*

called Intrepid: the secret war. Harcourt, Brace, Jovanovich, San Diego, CA, USA, 1976. ISBN 0-15-156795-6. xxv + 486 + 16 pp. LCCN D810.S8 S85.

Stern:1987:SLC

[Ste87] J. Stern. Secret linear congruential generators are not cryptographically secure. In IEEE [IEE87a], pages 421–426. ISBN 0-8186-0807-2, 0-8186-4807-4 (fiche), 0-8186-8807-6 (case). LCCN QA 76 S979 1987.

Stevens:1988:CPR

[Ste88] A. Stevens. C programming: off and running .... *Dr. Dobb's Journal of Software Tools*, 13(8):98, 101–102, 104, 106–107, 109–110, 113, August 1988. CODEN DDJOEB. ISSN 0888-3076.

Stephenson:1989:PPM

[Ste89] Peter Stephenson. Personal and private (microcomputer security). *BYTE Magazine*, 14(6):285–288, June 1989. CODEN BYTEDJ. ISSN 0360-5280.

Stevens:1990:CPi

[Ste90a] Al Stevens. C programming. *Dr. Dobb's Journal of Software Tools*, 15(9):127–??, September 1990. CODEN DDJOEB. ISSN 1044-789X.

Stevens:1990:CPk

[Ste90b] Al Stevens. C programming. *Dr. Dobb's Journal of Software Tools*, 15(11):149–??, November 1990. CODEN DDJOEB. ISSN 1044-789X.

Steinberg:1991:VSV

[Ste91] Steve Steinberg. Viewpoint: a student's view of cryptography in computer science. *Communications of the Association for Computing Machinery*, 34(2):15–17, February 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Stewart:1992:SCK

[Ste92] John N. Stewart. SunOS, C2 and Kerberos — a comparative review. In USENIX [USE92b], pages 265–284. ISBN 1-880446-46-4. LCCN ????

Stern:1994:DIS

[Ste94a] Jacques Stern. Designing identification schemes with keys of short size. In Desmedt [Des94b], pages 164–173. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390164.htm`; `http://link.springer-`

ny.com/link/service/series/0558/papers/0839/08390164.pdf.

Stevens:1994:PBa

[Ste94b] Al Stevens. Programmer's bookshelf. *Dr. Dobb's Journal of Software Tools*, 19(5): 141–??, May 1994. CODEN DDJOEB. ISSN 1044-789X.

Stern:1995:COD

[Ste95] J. Stern. Can one design a signature scheme based on error-correcting codes? *Lecture Notes in Computer Science*, 917:424–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stern:1996:VCA

[Ste96] J. Stern. The validation of cryptographic algorithms. *Lecture Notes in Computer Science*, 1163:301–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stern:1998:LCO

[Ste98a] J. Stern. Lattices and cryptography: An overview. *Lecture Notes in Computer Science*, 1431:50–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stern:1998:NEA

[Ste98b] J. P. Stern. A new and efficient all-or-nothing disclosure of secrets protocol. *Lecture Notes in Computer Science*, 1514:357–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stephenson:1999:C

[Ste99a] Neal Stephenson. *Cryptonomicon*. Avon Press, New York, 1999. ISBN 0-380-97346-4. ???? pp. LCCN PS3569.T3868 C79 1999. URL http://www.counterpane.com/solitaire.htm. Appendix by Bruce Schneier on "The Solitaire Encryption Algorithm", a secure OFB stream cipher that encrypts and decrypts using an ordinary deck of playing cards.

Stern:1999:ACE

[Ste99b] J. Stern, editor. *Advances in cryptology — EUROCRYPT '99: international conference on the theory and application of cryptographic techniques, Prague, Czech Republic, May 2–6, 1999; proceedings*, volume 1592 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-65889-0. LCCN QA76.9.A25 E964 1999.

Stern:1999:DU

[Ste99c] Jacques Stern. DFC update. In National Institute of Standards and Technology [Nat99b]. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Stinson:1991:CCA

[Sti91a] Douglas R. Stinson. Combinatorial characterizations of authentication codes. *Lecture Notes in Computer Science*, 576:62–73, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760062.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760062.pdf.

Stinson:1991:UHA

[Sti91b] Douglas R. Stinson. Universal hashing and authentication codes. *Lecture Notes in Computer Science*, 576:74–85, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760074.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760074.pdf.

Stinson:1993:NGL

[Sti93a] D. R. Stinson. New general lower bounds on the information rate of secret sharing schemes. *Lecture Notes in Computer Science*, 740:168–182, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stinson:1993:ACC

[Sti93b] Douglas R. Stinson, editor. *Advances in Cryptology, CRYPTO '93: 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22–26, 1993: Proceedings*, volume 773 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). LCCN QA76.9.A25 C79 1993.

Stinson:1994:ACC

[Sti94] Douglas R. Stinson, editor. *Advances in Cryptology, CRYPTO '93: 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22–26, 1993: Proceedings*, volume 773 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1993. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0773.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=773.

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:1998:C

[Sti98a] D. R. Stinson. Crypto '93. *Lecture Notes in Computer Science*, 1440: 159–164, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stinson:1998:VCT

[Sti98b] Doug Stinson. Visual cryptography and threshold schemes. *Dr. Dobb's Journal of Software Tools*, 23(4): 36, 38–43, April 1998. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/.

Stout:1965:DRN

[Sto65] Rex Stout. *The Doorbell Rang: a Nero Wolfe Novel*. ????, ????, 1965. ?? pp.

Stoll:1989:CET

[Sto89] Clifford Stoll. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday, New York, NY, USA, 1989. ISBN 0-385-24946-2, 0-307-81942-6 (e-book), 0-7434-1145-5, 0-7434-1146-3, 1-299-04734-3. vi + 326 pp. LCCN UB271.R92 H477 1989; UB271.R92 H4771 1989; UB271.R92 S47 1989. US$18.95. URL http://vxer.org/lib/pdf/The%20Cuckoo%27s%20Egg.pdf.

Stout:1990:SDE

[Sto90] Robert B. Stout. S-CODER for data encryption. *Dr. Dobb's Journal of Software Tools*, 15(1):52, 54, 56, 58, 110–111, January 1990. CODEN DDJOEB. ISSN 1044-789X.

Stone:1998:RBH

[Sto98] A. Stone. (re)butting heads over privacy. *IEEE Spectrum*, 35(7):10–13, July 1998. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Sivabalan:1993:DSN

[STP93] M. Sivabalan, S. Tavares, and L. E. Peppard. On the design of SP networks form an information theoretic point of view. *Lecture Notes in Computer Science*, 740:260–279, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stripp:1987:BJC

[Str87] Alan J. Stripp. Breaking Japanese codes. *Intelligence and National Security*, 2 (4):135–??, 1987. ISSN 0268-4527 (print), 1743-9019 (electronic).

Stripp:1989:CFE

[Str89] Alan Stripp. *Codebreaker in the Far East*. Cass series–studies in intelligence. F. Cass, London, England, 1989. ISBN 0-7146-3363-1. xiv + 204 pp. LCCN D810.C88 S76 1989.

Strauss:1993:SEC

[Str93a] P. Strauss. Secure E-mail cheaply with software encryption. *Datamation*, 39(23):48, December 1993. CODEN DTMNAT. ISSN 0011-6963.

Strauss:1993:SMC

[Str93b] P. Strauss. Secure E-mail cheaply with software encryption. *Datamation*, 39(23):48, December 1993. CODEN DTMNAT. ISSN 0011-6963.

Stripp:1995:CBF

[Str95] Alan Stripp. *Code Breaker in the Far East*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, second edition, 1995. ISBN 0-19-280386-7 (paperback), 0-19-285316-3. xiv + 204 pp. LCCN D810.C88 S76 1989.

Sander:1999:AAE

[STS99a] T. Sander and A. Ta-Shma. Auditable, anonymous electronic cash. In Wiener [Wie99], pages 555–572. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Sander:1999:FCN

[STS99b] T. Sander and A. Ta-Shma. Flow control: a new approach for anonymity control in electronic cash systems. In Franklin [Fra99], pages 46–61. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Sandholm:1999:DOC

[STSW99] T. Sandholm, S. Tai, D. Slama, and E. Walshe. Design of object caching in a CORBA OTM system. *Lecture Notes in Computer Science*, 1626:241–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stumme:1999:AEK

[Stu99] G. Stumme. Acquiring expert knowledge for the design of conceptual information systems. *Lecture Notes in Computer Science*, 1621:275–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Steiner:1995:REE

[STW95] Michael Steiner, Gene Tsudik, and Michael Waidner. Refinement and extension of encrypted key exchange. *Operating Systems Review*, 29(3):22–30, July 1995. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Su:1998:DEM

[Su98] Chang Ling Su. A data encryption method using variable-length codes. *Dongbei Shida Xuebao*, 2: 23–25, 1998. CODEN DSZKEE. ISSN 1000-1832.

Summers:1984:OCS

[Sum84] R. C. Summers. An overview of computer security. *IBM Systems Journal*, 23(4):309–325, 1984. CODEN IBMSA7. ISSN 0018-8670.

Sun:1991:UDE

[Sun91a] Qi Sun. Using Diophantine equations to construct public key cryptosystems. *Sichuan Daxue Xuebao*, 28 (1):15–18, 1991. CODEN SCTHAO. ISSN 0490-6756.

Sun:1991:RSE

[Sun91b] Sun Microsystems Computer Corporation. A release of Solaris 1.0.1 encryption kit for SunOS 4.1.2 for SPARC systems, 1991.

Sun:1998:ISM

[Sun98a] H.-M. Sun. Improving the security of the McEliece public-key cryptosystem. *Lecture Notes in Computer Science*, 1514:200–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sundsted:1998:SDI

[Sun98b] Todd Sundsted. Signed and delivered: An introduction to security and authentication. *JavaWorld: IDG's magazine for the Java community*, 3(12): ??, 1998. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/jw-12-1998/jw-12-howto.htm`.

SuperMacSoftware:1988:SDE

[Sup88] SuperMac Software. Sentinel Data encryption utility, 1988.

Sutoh:1999:HPP

[Sut99] Hiroki Sutoh. A high-performance public key cryptography co-processor for super multi-purpose smart card. In Anonymous [Ano99c], page ??

Shand:1993:FIR

[SV93] M. Shand and J. Vuillemin. Fast implementations of RSA cryptography. In Swartzlander, Jr. et al. [SIJ93], pages 252–259. ISBN 0-7803-1401-8 (softbound), 0-8186-3862-1 (casebound), 0-8186-3861-3 (microfiche). ISSN 0018-9340 (print), 1557-9956 (electronic). LCCN QA 76.9 C62 S95 1993. URL `http://www.acsel-lab.com/arithmetic/arith11/papers/ARITH11_Shand.pdf`. IEEE Transactions on Computers **43(8)**, 1994.

Schnorr:1994:BBC

[SV94] Claus Peter Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. Technical report TR-94-017, International Computer Science Institute, Berkeley, CA, USA, April 1994. xi pp.

Schnorr:1995:BBC

[SV95a] C. P. Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. *Lecture Notes in Computer Science*, 950:47–57, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shepherd:1995:GJ

[SV95b] S. J. Shepherd and P. W. J. Van Eetvelt. On goats and jammers. *Bulletin of the IMA*, 31(5–6):87–89, May 1995.

Stern:1998:CC

[SV98] Jacques Stern and Serge Vaudenay. CS-CIPHER. *Lecture Notes in Computer Science*, 1372:189–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720189.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1372/13720189.pdf`.

Shamir:1999:PHS

[SV99a] A. Shamir and N. Van Someren. Playing 'hide and seek' with stored keys. *Lecture Notes in Computer Science*, 1648:118–124, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shamir:1999:PSS

[SV99b] A. Shamir and N. Van Someren. Playing 'hide and seek' with stored keys. In Franklin [Fra99], pages 118–124. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Samuels:1998:LSA

[SvA+98] Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling PC's; server-side scripting; stronger encryption; inner loops; Einstein kudos. *Dr. Dobb's Journal of Software Tools*, 23(3):8, 12, March 1998. CODEN DDJOEB. ISSN 1044-789X.

Sivakumar:1999:PPN

[SVB99] R. Sivakumar, N. Venkitaraman, and V. Bharghavan. The Protean Programmable Network Architecture: Design and initial experience. *Lecture Notes in Computer Science*, 1653:37–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shepherd:1996:SAD

[SVBJ96] S. J. Shepherd, P. W. J. Van Eetvelt, S. K. Barton, and I. R. Johnson. Simulation and analysis of the distortion generated by the bulk-FFT demultiplexer. *Journal of Signal Processing*, 54(??): 285–294, ???? 1996.

Shamir:1998:PHS

[SvS98] Adi Shamir and Nicko van Someren. Playing hide and seek with stored keys. Technical report, Applied Math Dept., The Weizmann Institute of Science, Rehovot 76100, Israel, and nCipher Corporation Limited, Cambridge, England, September 22, 1998. URL `????/keyhide2.pdf`.

Shepherd:1995:SCS

[SVWMB95] S. J. Shepherd, P. W. J. Van Eetvelt, C. W. Wyatt-Millington, and S. K. Barton. A simple coding scheme to reduce peak factor in QPSK multi-carrier modulation. *Electronics Letters*, 31(14):1131–1132, July 1995. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic).

Smeets:1991:CAC

[SVxW91] Ben Smeets, Peter Vanroose, and Zhe xian Wan. On the construction of authentication codes with sand codes withstanding spoofing attacks of order $L \geq 2$. *Lecture Notes in Computer Science*, 473: 306–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730306.htm; http://link.springer-ny.com/link/service/series/`

0558/papers/0473/04730306.pdf.

Shulman:1961:GC

[SW61] David Shulman and Joseph Weintraub. *A glossary of cryptography*. Handbook of cryptography; section 1. Crypto Press, New York, NY, USA, 1961. various pp. LCCN Z103 .S48.

Smith:1983:HCR

[SW83] J. W. Smith and S. S. Wagstaff, Jr. How to crack an RSA cryptosystem. *Congressus Numerantium*, 40: 367–373, 1983. ISSN 0384-9864.

Silverman:1993:PAE

[SW93] R. D. Silverman and S. S. Wagstaff, Jr. A practical analysis of the elliptic curve factoring algorithm. *Mathematics of Computation*, 61: 445–462, 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Saeki:1994:SSS

[SW94a] M. Saeki and K. Wenyin. Specifying software specification and design methods. *Lecture Notes in Computer Science*, 811:353–366, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Safford:1994:UNC

[SW94b] Laurance F. Safford and J. N. Wenger. *U.S. naval communications intelligence activities*, volume 65 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1994. ISBN 0-89412-229-0. v + 85 pp. LCCN VB230 .S24 1994. Comprised of especially edited versions of SRH-149, SRH-150, SRH-151, SRH-152, and SRH-197, now declassified documents in the National Archives, Washington, DC.

Snow:1994:SA

[SW94c] C. R. Snow and H. Whitfield. Simple authentication. *Software—Practice and Experience*, 24(5):437–447, May 1994. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Scheidler:1995:PKC

[SW95a] Renate Scheidler and Hugh C. Williams. A public-key cryptosystem utilizing cyclotomic fields. *Designs, Codes, and Cryptography*, 6 (2):117–131, 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Stansfield:1995:CCS

[SW95b] E. V. Stansfield and M. Walker. Coding and cryptography for speech and vision. *Lecture Notes in Computer Science*, 1025:213–??, 1995. CODEN LNCSD9. ISSN

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

Schneier:1997:FSEa

[SW97a] B. Schneier and D. Whiting. Fast software encryption: Designing encryption algorithms for optimal software speed on the Intel Pentium processor. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1997. 18 pp. URL http://www.counterpane.com/fast_software_encryption.html. Also published in *Fast Software Encryption, Fourth International Workshop Proceedings (January 1997)*, Springer-Verlag, 1997, pp. 242–259 [SW97b].

Schneier:1997:FSEb

[SW97b] Bruce Schneier and Doug Whiting. Fast software encryption: Designing encryption algorithms for optimal software speed on the Intel Pentium processor. *Lecture Notes in Computer Science*, 1267:242–259, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670242.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670242.pdf; http://www.counterpane.com/fast_software_encryption.html.

Stinson:1998:ARS

[SW98] D. R. (Douglas Robert) Stinson and R. Wei. An application of ramp schemes to broadcast encryption. Research report CORR 98-02, Faculty of Mathematics, University of Waterloo, Waterloo, ON, Canada, 1998. 7 pp.

Stinson:1999:ARS

[SW99a] D. R. Stinson and R. Wei. An application of ramp schemes to broadcast encryption. *Information Processing Letters*, 69(3):131–135, February 12, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Stinson:1999:KPT

[SW99b] D. R. Stinson and R. Wei. Key preassigned traceability schemes for broadcast encryption. *Lecture Notes in Computer Science*, 1556: 144–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Swan:1994:AAb

[Swa94] Tom R. Swan. Algorithm alley. *Dr. Dobb's Journal of Software Tools*, 19(2):103–??, February 1994. CODEN DDJOEB. ISSN 1044-789X.

Swire:1997:ULF

[Swi97] P. P. Swire. The uses and limits of financial cryptography: a law professor's perspective. *Lecture Notes in Computer Science*, 1318: 239–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Salzer:1981:RHH

[SWT+81] Herbert E. Salzer, Eric A. Weiss, Henry S. Tropp, Jane Smith, and Robert W. Rector. Reviews: H. H. Goldstine: A History of Numerical Analysis; Electronics: An Age of Innovation; J. A. N. Lee: Banquet Anecdotes and Conference Excerpts; R. L. Wexelblat: History of Programming Languages: Capsule reviews. *Annals of the History of Computing*, 3(3):289–302, July/ September 1981. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1981/pdf/a3289.pdf; http://www.computer.org/annals/an1981/a3289abs.htm. See minor correction [Ano81a].

Sun:1989:TKE

[SX89] Qi Sun and Rong Xiao. Two kinds of elliptic curves over F_q used to set up cryptosystems. *Sichuan Daxue Xuebao*, 26(1):39–43, 1989. CODEN SCTHAO. ISSN 0490-6756.

Sun:1990:KGE

[SX90] Qi Sun and Rong Xiao. A kind of good elliptic curve used to set up cryptosystem. *Chinese Sci. Bull.*, 35 (1):81–82, 1990. ISSN 1001-6538.

Salomaa:1986:PCB

[SY86a] A. Salomaa and S. Yu. On a public-key cryptosystem based on iterated morphisms and substitutions. *Theoretical Computer Science*, 48(2-3):283–296, ???? 1986. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Salomaa:1986:PKC

[SY86b] Arto Salomaa and Sheng Yu. On a public-key cryptosystem based on iterated morphisms and substitutions. *Theoretical Computer Science*, 48(2-3):283–296 (1987), 1986. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Smith:1992:ICF

[SY92] R. M. Smith, Sr. and P. C. Yeh. Integrated Cryptographic Facility of the Enterprise Systems Architecture/390: design considerations. *IBM Journal of Research and Development*, 36(4):683–693, July 1992.

CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Sakurai:1996:BDB

[SY96a] K. Sakurai and Y. Yamane. Blind decoding, blind undeniable signatures, and their applications to privacy protection. In Anderson [And96c], pages 257–264. CODEN LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I5414 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054625.html`.

Shieh:1996:AKD

[SY96b] Shiuh-Pyng Shieh and Wen-Her Yang. An authentication and key distribution system for open network systems. *Operating Systems Review*, 30(2):32–41, April 1996. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Sowers:1998:TDW

[SY98] Sabrina Sowers and Abdou Youssef. Testing digital watermark resistance to destruction. *Lecture Notes in Computer Science*, 1525:239–257, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250239.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1525/15250239.pdf`.

Sellini:1999:VKV

[SY99] F. Sellini and P.-A. Yvars. Veri-KoMoD: Verification of knowledge models in the mechanical design field. *Lecture Notes in Computer Science*, 1621:385–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sakurai:1998:KES

[SYMI98] K. Sakurai, Y. Yamane, S. Miyazaki, and T. Inoue. A key escrow system with protecting user's privacy by blind decoding. *Lecture Notes in Computer Science*, 1396:147–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Syverson:1992:KBS

[Syv92] Paul F. Syverson. Knowledge, belief, and semantics in the analysis of cryptographic protocols. *Journal of Computer Security*, 1 (3–4):317–334, ???? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Syverson:1993:KDP

[Syv93] Paul Syverson. On key distribution protocols for repeated authentication. *Operating Systems Review*, 27 (4):24–30, October 1993. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Seberry:1993:ACA

[SZ93] Jennifer Seberry and Yuliang Zheng, editors. *Advances in cryptology — AUSCRYPT '92: Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13–16, 1992: proceedings*, volume 718 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. CODEN LNCSD9. ISBN 0-387-57220-1 (New York), 3-540-57220-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 A87 1992.

Sakurai:1996:CWR

[SZ96] K. Sakurai and Y. Zheng. Cryptographic weaknesses in the round transformation used in a block cipher with provable immmunity against linear cryptanalysis. *Lecture Notes in Computer Science*, 1178:376–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Szepietowski:1998:WSO

[Sze98] Andrzej Szepietowski. Weak and strong one-way space complexity classes. *Information Processing Letters*, 68(6):299–302, December 30, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Swanson:1996:RDH

[SZT96a] M. D. Swanson, B. Zhu, and A. H. Tewfik. Robust data hiding for images. In Lervik and Waldemar [LW96], pages 37–40. ISBN 0-7803-3629-1 (softbound), 0-7803-3630-5 (microfiche), 82-993923-0-6 (Norway) (??invalid checksum??). LCCN TK5102.9.I3 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1035.html`. IEEE catalog number: 96TH8225.

Swanson:1996:TRI

[SZT96b] M. D. Swanson, B. Zhu, and A. H. Tewfik. Transparent robust image watermarking. In IEEE [IEE96e], pages 211–214. ISBN 0-7803-3258-X (softbound), 0-7803-3259-8 (casebound), 0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM). LCCN TK8315.I222 1996. URL `http://www.cl.cam.`

ac.uk/~fapp2/steganography/bibliography/1037.html. Three volumes. IEEE catalog number 96CH35919.

Swanson:1998:MSB

[SZT98a] M. D. Swanson, B. Zhu, and A. H. Tewfik. Multiresolution scene-based video watermarking using perceptual models. *IEEE Journal on Selected Areas in Communications*, 16(4): 540–550, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072157.html.

Swanson:1998:MSV

[SZT98b] Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewfik. Multiresolution scene-based video watermarking using perceptual models. *IEEE Journal on Selected Areas in Communications*, 16(4):540–550, May 1998. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic).

Swanson:1998:RAW

[SZTB98] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney. Robust audio watermarking using perceptual masking. *Signal Processing*, 66(3):337–355, May 1998. CODEN SPRODR. ISSN 0165-1684. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073173.html.

Szweda:1997:ECF

[Szw97a] Roy Szweda. Encrypted communications frustrate FBI. *Network Security*, 1997(10):4, October 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897900994.

Szweda:1997:ESW

[Szw97b] Roy Szweda. Encryption software for Windows. *Network Security*, 1997(7): 8, July 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897898777.

Szweda:1997:STF

[Szw97c] Roy Szweda. Sun takes on Feds over US encryption regulations. *Network Security*, 1997(7): 6, July 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897898704.

Seberry:1994:ISA

[SZZ94a] Jennifer Seberry, Xian Mo Zhang, and Yuliang Zheng. Improving the strict avalanche characteristics of cryptographic functions. *Information Processing Letters*, 50(1):37–41, April 8, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Seberry:1994:PDS

[SZZ94b] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Pitfalls in designing substitution boxes. In Desmedt [Des94b], pages 383–396. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390383.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390383.pdf.

Seberry:1995:RAN

[SZZ95a] J. Seberry, X.-M. Zhang, and Y. Zheng. Relationships among nonlinearity criteria. *Lecture Notes in Computer Science*, 950: 376–388, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Seberry:1995:SCF

[SZZ95b] J. Seberry, X.-M. Zhang, and Y. Zheng. Structures of cryptographic functions with strong avalanche characteristics. *Lecture Notes in Computer Science*, 917: 119–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Seberry:1995:RBP

[SZZ95c] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. The relationship between propagation characteristics and nonlinearity of cryptographic functions. *J.UCS: Journal of Universal Computer Science*, 1(2):136–150, February 28, 1995. ISSN 0948-6968. URL http://www.iicm.edu/jucs_1_2/the_relationship_between_propagation.

Theodoridis:1998:NES

[T+98] S. Theodoridis et al., editors. *Signal processing IX, theories and applications: proceedings of Eusipco-98, Ninth European Signal Processing Conference, Rhodes, Greece, 8–11 September 1998*. Typorama Editions, Patras, Greece, 1998. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. Four volumes.

Takano:1999:CAC

[T+99] Kohji Takano et al. A cryptographic accelerator card with small fast low-power RSA engines. In Anonymous [Ano99c], page ??

Tardo:1992:SGA

[TA92] Joseph J. Tardo and Kannan Alagappan. SPX: Global authentication using public key certificates. *Journal of Computer Security*, 1(3–4):295–316, ???? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Tang:1997:DBC

[TA97] Weili Tang and Yoshinao Aoki. DCT-based coding of images in watermarking. In IEEE [IEE97k], pages 510–512. ISBN 0-7803-3676-3 (softbound,) 0-7803-3677-1 (microfiche). LCCN TK5102.9.I546 1997. Three volumes. IEEE catalog number: 97TH8237.

Taaffe:1998:NBL

[Taa98] Joanne Taaffe. News: Bull to launch Java smart card. *JavaWorld: IDG's magazine for the Java community*, 3(1):??, January 1998. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/jw-01-1998/jw-01-idgns.smartcard.htm`.

Tabatabaian:1994:CAP

[Tab94] Seyed Jalil Tabatabaian. *Cryptanalysis algorithms for public key cryptosystems*. Thesis (Ph.D.), University of Newcastle upon Tyne, Newcastle upon Tyne, UK, 1994. xxi + 322 pp.

Takagi:1997:FRT

[Tak97] Tsuyoshi Takagi. Fast RSA-type cryptosystems using n-adic expansion. *Lecture Notes in Computer Science*, 1294:372–384, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940372.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940372.pdf`.

Takagi:1998:FRC

[Tak98a] T. Takagi. Fast RSA-type cryptosystem modulo $p^k q$. *Lecture Notes in Computer Science*, 1462:318–326, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Takagi:1998:FRT

[Tak98b] Tsuyoshi Takagi. Fast RSA-type cryptosystem modulo $p^k q$. *Lecture Notes in Computer Science*, 1462:318–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http:/`

/link.springer-ny.com/link/service/series/0558/bibs/1462/14620318.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620318.pdf.

Tanaka:1990:RSI

[Tan90] Hatsukazu Tanaka. A realization scheme for the identity-based cryptosystem. *Electronics and communications in Japan. Part 3, Fundamental electronic science*, 73(5):1–7, 1990. CODEN ECJSER. ISSN 1042-0967 (print), 1520-6440 (electronic).

Tao:1994:FAO

[Tao94] Renji Tao. On finite automaton one-key cryptosystems. *Lecture Notes in Computer Science*, 809: 135–148, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tardo:1990:PKB

[TAP90] Joe Tardo, Kannan Alagappan, and Richard Pitkin. Public-key-based authentication using Internet certificates. In USENIX Association [USE90], pages 121–124. LCCN QA 76.9 A25 U55 1990.

TFEC:1998:CPF

[Tas98] Task Force on Electronic Commerce. *A cryptography policy framework for electronic commerce: building Canada's information economy and society*. Ottawa, ON, Canada, 1998. 35 + 38 pp. Distributed by the Government of Canada Depository Services Program. Text in English and French on inverted pages. Title of the French text: Politique cadre en matière de cryptographie aux fins du commerce électronique. Available also on the Internet.

Tattersall:1998:ENT

[Tat98] James J. (James Joseph) Tattersall. *Elementary number theory in nine chapters*. Cambridge University Press, Cambridge, UK, 1998. ISBN 0-521-58503-1 (hardback), 0-521-58531-7 (paperback). ???? pp. LCCN QA241 .T35 1998.

Tattersall:1999:ENT

[Tat99] James J. (James Joseph) Tattersall. *Elementary number theory in nine chapters*. Cambridge University Press, Cambridge, UK, 1999. ISBN 0-521-58503-1 (hardcover), 0-521-58531-7 (paperback), 0-511-75635-6 (e-book). viii + 407 pp. LCCN QA241 .T35 1998.

Taylor:1990:DSI

[Tay90] Laura Mignon Taylor. Data security issues and encryption algorithms. Thesis

(M.S.), University of Colorado, Boulder, CO, USA, 1990. vii + 131 pp.

Taylor:1994:ICV

[Tay94] Richard Taylor. An integrity check value algorithm for stream ciphers. *Lecture Notes in Computer Science*, 773:40–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Taylor:1995:NOU

[Tay95] Richard Taylor. Near optimal unconditionally secure authentication. *Lecture Notes in Computer Science*, 950:244–253, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500244.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500244.pdf`.

Tao:1985:FAP

[TC85] Ren Ji Tao and Shi Hua Chen. A finite automaton public key cryptosystem and digital signatures. *Chinese Journal of Computers = Chi suan chi hsueh pao*, 8 (6):401–409, 1985. CODEN JIXUDT. ISSN 0254-4164.

Tao:1986:TVF

[TC86] Ren Ji Tao and Shi Hua Chen. Two varieties of finite automaton public key cryptosystem and digital signatures. *Journal of computer science and technology*, 1 (1):9–18, 1986. CODEN JCTEEM. ISSN 1000-9000.

Tsujii:1991:NIB

[TC91] Shigeo Tsujii and Jinhui Chao. A new ID-based key sharing system. *Lecture Notes in Computer Science*, 576:288–299, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tao:1997:VPK

[TC97] Renji Tao and Shihua Chen. A variant of the public key cryptosystem FAPKC3. *Journal of Network and Computer Applications*, 20 (3):283–303, July 1997. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804597900576`.

Tao:1999:GPK

[TC99a] Renji Tao and Shihua Chen. The generalization of public key cryptosystem FAPKC4. *Chinese Sci. Bull.*, 44(9): 784–789, 1999. ISSN 1001-6538.

Tao:1999:FAP

[TC99b] Renji Tao and Shihua Chen. On finite automaton public-key cryptosystem. *Theoretical Computer Science*, 226(1–2):143–172, September 17, 1999. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1999&volume=226&issue=1-2&aid=3231.

Tao:1997:FNF

[TCC97] Renji Tao, Shihua Chen, and Xuemei Chen. FAPKC3: a new finite automaton public key cryptosystem. *Journal of computer science and technology*, 12(4):289–305, 1997. CODEN JCTEEM. ISSN 1000-9000.

Tangney:1991:SIS

[TCH+91] Brendan Tangney, Vinny Cahill, Chris Horn, Dominic Herity, Alan Judge, Gradimir Starovic, and Mark Sheppard. Some ideas on support for fault tolerance in COMANDOS, an object oriented distributed system. *Operating Systems Review*, 25(2):130–135, April 1991. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Tedrick:1985:FES

[Ted85] Tom Tedrick. Fair exchange of secrets (extended abstract). In Blakley and Chaum [BC85], pages 434–438. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=434. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Teske:1998:SPR

[Tes98] E. Teske. Speeding up Pollard's rho method for computing discrete logarithms. *Lecture Notes in Computer Science*, 1423: 541–554, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

TI:1984:TTU

[Tex84] Texas Instruments Inc. *TMS7500 TMS75C00 user's guide, data encryption device: 8-bit microcomputer family*. Texas Instruments, Dallas, TX, USA, 1984. various pp.

Tourigny:1994:DSD

[TG94] Yves Tourigny and Michael Grinfeld. Deciphering singularities by discrete methods. *Mathematics of Computation*, 62(205):155–169, January 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Tanaka:1999:PCD

[TGKI99] Y. Tanaka, N. Goto, M. Kakei, and T. Inoue. Parallel computational design of NJR global climate models. *Lecture Notes in Computer Science*, 1615: 281–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tzeng:1999:IPI

[TH99] Wen-Guey Tzeng and Chi-Ming Hu. Inter-protocol interleaving attacks on some authentication and key distribution protocols. *Information Processing Letters*, 69(6):297–302, March 26, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Thao:1991:SAD

[Tha91] Sam V. Thao. A statistical analysis of the data encryption standard. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1991. viii + 58 pp.

Theobald:1995:HBS

[The95] T. Theobald. How to break Shamir's asymmetric basis. *Lecture Notes in Computer Science*, 963:136–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Thomas:1974:RPS

[Tho74] R. Thomas. RFC 644: On the problem of signature authentication for network mail, July 22, 1974. URL `ftp://ftp.internic.net/rfc/rfc644.txt`; `ftp://ftp.math.utah.edu/pub/rfc/rfc644.txt`. Status: UNKNOWN. Not online.

Thompson:1984:RTT

[Tho84] Ken Thompson. Reflections on trusting trust. *Communications of the Association for Computing Machinery*, 27(8):761–763, August 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1028.html`.

Thomas:1986:SDE

[Tho86] John A. Thomas. Survey of data encryption in DOL. *Dr. Dobb's Journal of Software Tools*, 11(6):16–??, June 1986. CODEN DDJOEB. ISSN 1044-789X.

Thompson:1987:RTT

[Tho87] Ken Thompson. Reflections on trusting trust. In Ashenhurst [Ash87], page ?? ISBN 0-201-07794-9. LCCN QA76.24 .A33 1987. ACM Turing Award lecture.

Thomas:1996:PVS

[Tho96] Craig C. Thomas. Privacy vs. security: values and the encryption debate. Thesis (M.A.), Georgetown University, Washington, DC, USA, 1996. v + 82 pp.

Tarman:1998:AAE

[THP+98] Thomas D. Tarman, Robert L. Hutchinson, Lyndon G. Pierson, Peter E. Sholander, and Edward L. Witzke. Algorithm-agile encryption in ATM networks. *Computer*, 31(9):57–64, September 1998. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `http://computer.org/computer/r9057abs.htm`; `http://dlib.computer.org/co/books/co1998/pdf/r9057.pdf`.

Tsujii:1988:PKC

[TIF+88] Shigeo Tsujii, Toshiya Itoh, Atsushi Fujioka, Kaoru Kurosawa, and Tsutomu Matsumoto. A public-key cryptosystem based on the difficulty of solving a system of nonlinear equations. *Systems and computers in Japan*, 19(2):10–18, 1988. CODEN SCJAEP. ISSN 0882-1666.

Tilki:1998:EHD

[Til98] John F. Tilki. Encoding a hidden digital signature using psychoacoustic masking. Thesis (M.S.), Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, 1998.

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. Reprinted in 1952. Reprinted in 1959 with a foreword by Karl Pearson.

Taaffe:1997:NSL

[TJ97] Joanne Taaffe and Margret Johnston. News: Siemens licenses Java for smart cards. *JavaWorld: IDG's magazine for the Java community*, 2(8):??, August 1997. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/jw-08-1997/jw-08-idgns.smartcards.htm`.

Tseng:1999:ATS

[TJ99] Yuh-Min Tseng and Jinn-Ke Jan. Attacks on threshold signature schemes with traceable signers. *Information Processing Letters*, 71(1):1–4, July 16, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Takagi:1999:DRA

[TK99] N. Takagi and S. Kuwahara. Digit-recurrence algorithm for computing Euclidean norm of a 3-D vector. In Koren and Kornerup [KK99b], pages 86–95. ISBN 0-7803-5609-8, 0-7695-0116-8, 0-7695-0118-4. ISSN 1063-6889. LCCN QA76.6 .S887 1999. URL `http://euler.ecs.umass.edu/paper/final/paper-142.pdf; http://euler.ecs.umass.edu/paper/final/paper-142.ps`. IEEE Computer Society Order Number PR00116. IEEE Order Plan Catalog Number 99CB36336.

Tzovaras:1998:RIW

[TKS98] D. Tzovaras, N. Karagiannis, and M. G. Strintzis. Robust image watermarking in the subband or discrete cosine transform domain. In Theodoridis et al. [T+98], pages 2285–2288. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073179.html`. Four volumes.

Theodoratos:1999:DGD

[TLS99] D. Theodoratos, S. Ligoudistianos, and T. Sellis. Designing the global data warehouse with SPJ views. *Lecture Notes in Computer Science*, 1626:180–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tavares:1999:SAC

[TM99] Stafford Tavares and Henk Meijer, editors. *Selected areas in cryptography: 5th annual International Workshop, SAC '98, Kingston, Ontario, Canada, August 17–18, 1998: proceedings*, volume 1556 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-65894-7 (softcover). LCCN QA76.9.A25 S22 1998.

Takagi:1996:MMP

[TN96a] T. Takagi and S. Naito. The multi-variable modular polynomial and its applications to cryptography. *Lecture Notes in Computer Science*, 1178:386–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Takagi:1996:MVM

[TN96b] T. Takagi and S. Naito. The multi-variable modular polynomial and its applications to cryptography. *Lecture Notes in Computer Science*, 1178:386–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Terada:1997:LDC

[TN97] Routo Terada and Jorge Nakahara. Linear and differential cryptanalysis of FEAL-N with swapping. Relatorio tecnico RT-MAC-9709, Universidade de Sao Paulo, Instituto de Matematica e Estatistica, São Paulo, Brasil, September 1997. 10 pp.

Todorovic:1997:CAS

[Tod97] B. M. Todorovic. Code acquisition scheme for frequency hopping radio in channels with fading. *Electronics Letters*, 33(3):177–179, January 30, 1997. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061459.html`.

Tirkel:1998:IWR

[TOH98] A. Z. Tirkel, C. F. Osborne, and T. E. Hall. Image and watermark registration. *Signal Processing*, 66(3):373–383, May 1998. CODEN SPRODR. ISSN 0165-1684. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073176.html`.

Tonchev:1996:CDG

[Ton96] Vladimir Tonchev. *Codes, designs, and geometry.* Kluwer Academic Publishers, Dordrecht, The Netherlands, 1996. ISBN 0-7923-9759-2. 120 pp. LCCN QA166.25 .C63 1996. A special issue of Designs, codes and cryptography, an international journal, volume 9, no. 1 (1996).

Toussaint:1991:DCK

[Tou91] Marie-Jeanne Toussaint. Deriving the complete knowledge of participants in cryptographic protocols (extended abstract). *Lecture Notes in Computer Science*, 576:24–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760024.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0576/05760024.pdf`.

Toussaint:1992:SSI

[Tou92] Marie-Jeanne Toussaint. Separating the specification and implementation phases in cryptology. *Lecture Notes in Computer Science*, 648:77–??, 1992. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic).

Toussaint:1993:FVP

[Tou93] Marie-Jeanne Toussaint. Formal verification of probabilistic properties in cryptographic protocols. *Lecture Notes in Computer Science*, 739:412–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tsunoo:1994:COA

[TOU94] Yukiyasu Tsunoo, Eiji Okamoto, and Tomohiko Uyematsu. Ciphertext only attack for one-way function of the MAP using one ciphertext. In Desmedt [Des94b], pages 369–382. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390369.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0839/08390369.pdf`.

Touch:1995:RRM

[Tou95] J. Touch. RFC 1810: Report on MD5 performance, June 1995. URL `ftp://ftp.internic.net/rfc/rfc1810.txt`; `https://www.math.utah.edu/pub/rfc/rfc1810.txt`. Status: INFORMATIONAL.

Townsend:1998:QCO

[Tow98] P. D. Townsend. Quantum cryptography on optical fiber networks. *Lecture Notes in Computer Science*, 1470:35–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Thompson:1963:SDE

[TP63] James Westfall Thompson and Saul Kussiel Padover. *Secret diplomacy; espionage and cryptography, 1500-1815*. F. Ungar Pub. Co, New York, NY, USA, 1963. 290 pp. LCCN JX1648 .T5 1963. “Appendix: Cryptography”: p. 253–263. Bibliography: p. 265–282.

Traore:1997:MUF

[Tra97] J. Traore. Making unfair a “fair” blind signature scheme. *Lecture Notes in Computer Science*, 1334: 386–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Traore:1999:GST

[Tra99] J. Traore. Group signatures and their relevance to privacy-protecting offline electronic cash systems. *Lecture Notes in Computer Science*, 1587: 228–243, 1999. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tremblett:1999:JPA

[Tre99] Paul Tremblett. The Java provider architecture. *Dr. Dobb's Journal of Software Tools*, 24(3):40, 42, 44–47, 49, March 1999. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/1999/9902/9902toc.htm`; `http://www.ddj.com/ftp/1999/1999_03/provider.txt`; `http://www.ddj.com/ftp/1999/1999_03/provider.zip`.

Trithemius:1518:PLS

[Tri18] Johannes Trithemius. *Polygraphiae Libri Sex*. ????, ????, 1518. ???? pp.

Trithemius:1606:CGT

[Tri06a] Johannes Trithemius. *Clauis generalis triplex in libros steganographicos Iohannis Trithemij ...*. Iohannis Berneri, Frankfurt, Germany, 1606. 7 + 1 pp. LCCN Z103.T84 S 1606. Ab ipso authore conscripta ... Darmbstadij: Excudebat Balthasar Hofmann, impensis Iohannis Berneri, bibliop. Francof., anno 1606.

Trithemius:1606:CSI

[Tri06b] Johannes Trithemius. *Clauis Steganographiae Ioannis Trithemij, abbatis Spanheimensis, ad Serenissimum Principem Dn. Philippum ...*. Ioannem Bernerum, Frankfurt, Germany, 1606. 70 pp. LCCN Z103.T84 S 1606. Venundatur apud Ioannem Bernerum, bibliopolam Francofurtensem, anno 1606.

Trithemius:1606:SHE

[Tri06c] Johannes Trithemius. *Steganographia: hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*. Matthiae Beckeri, Frankfurt, Germany, 1606. 8 + 180 pp. LCCN Z103.T84 S 1606. Authore ... Ioanne Trithemio ...; praefixa est huic operi sua clauis, seu vera introductio ab ipso authore concinnata ... nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta. Francofurti. Ex officina typographica Matthiae Beckeri, sumptibus Ioannis Berneri, anno 1606.

Trithemius:1621:CGT

[Tri21a] Johannes Trithemius. *Clauis generalis triplex in libros steganographicos Iohannis Trithemij ...*. Balthasar Hofmann, Darmstadt, Germany, 1621. 7 + 1 pp. LCCN Z103 .T84 1621. Ab ipso authore conscripta ... Darmbstadij. Excudebat Balthasar Hofmann, impensis Iohannis Berneri, bibliop. Francof., anno 1621.

Trithemius:1621:CSI

[Tri21b] Johannes Trithemius. *Clauis Steganographiae Ioannis Trithemij, abbatis Spanheimensis, ad Serenissimum Principem Dn. Philippum ....* Iohannem Bernerum, Frankfurt, Germany, 1621. 64 pp. LCCN Z103 .T84 1621. Venundatur apud Iohannem Bernerum, bibliopolam Francofurtensem, anno 1621.

Trithemius:1621:SHE

[Tri21c] Johannes Trithemius. *Steganographia: hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*. Balthasaris Aulaeandri, Darmstadt, Germany, 1621. 8 + 152 + 2 pp. LCCN Z103 .T84 1621. Authore ... Ioanne Trithemio ...; praefixa est huic operi sua clauis, seu vera introductio ab ipso authore concinnata ... nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta. Darmbstadij. Ex officina typographica Balthasaris Aulaeandri, sumptibus vero Ioannis Berneri, bibliop. Francof., anno 1621.

Trostle:1993:MFT

[Tro93] J. T. Trostle. Modelling a fuzzy time system. In IEEE [IEE93b], pages 82–89. ISBN 0-8186-3370-0 (paperback), 0-8186-3371-9 (microfiche), 0-8186-3372-7 (casebound). LCCN QA 76.9 A25 I34 1993. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/023217.html`. IEEE catalog number 93CH3290-4.

Tronson:1997:C

[Tro97] Jennifer Tronson. Cryptology. Thesis (B.S.), California Polytechnic State University, San Luis Obispo, CA, USA, 1997. iii + 31 pp.

Tirkel:1993:EW

[TRS+93] A. Z. Tirkel, G. A. Rankin, Van Schyndel, R. M., W. J. Ho, N. R. A. Mee, and C. F. Osborne. Electronic watermark. In Kit and Ginige [KG93], pages 666–673. ISBN 0-646-16522-4. LCCN ???? URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1051.html`. Two volumes. Second biennial conference of the Australian Pattern Recognition Society.

Terry:1988:MSV

[TS88] Douglas B. Terry and Daniel C. Swinehart. Managing stored voice in the Etherphone system. *ACM Transactions on Computer Systems*, 6(1):3–27, February 1988. CODEN ACSYEC. ISSN 0734-2071. URL http://www.acm.org:80/pubs/citations/journals/tocs/1988-6-1/p3-terry/.

Tso:1990:NPK

[Ts'90] Theodore Ts'o. Nox, a private key encryption server with flexible semantics. Thesis (B.S.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1990. 49 pp. Supervised by David Clark.

Tso:1997:MEE

[Ts'97] Theodore Ts'o. Microsoft 'embraces and extends' Kerberos V5. *;login: the USENIX Association newsletter*, 22(6):??, November 1997. CODEN LOGNEM. ISSN 1044-6397. URL http://www.usenix.org/publications/login/1997-11/embraces.html.

Tokita:1995:LCL

[TSM95] T. Tokita, T. Sorimachi, and M. Matsui. Linear cryptanalysis of LOKI and s02DES. *Lecture Notes in Computer Science*, 917: 293–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tombak:1993:ACP

[TSN93] L. Tombak and R. Safavi-Naini. Authentication codes with perfect protection. *Lecture Notes in Computer Science*, 718:15–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tsudik:1989:DAI

[Tsu89] G. Tsudik. Datagram authentication in Internet gateways: Implications of fragmentation and dynamic routing. *IEEE Journal on Selected Areas in Communications*, 7(4):499–??, May 1, 1989. CODEN ISACEM. ISSN 0733-8716.

Tsudik:1992:MAOb

[Tsu92a] G. Tsudik. Message authentication with one-way hash functions. In IEEE [IEE92d], page ?? Three volumes. IEEE Computer Society order number 2860. IEEE catalog number 92CH3133-6.

Tsudik:1992:MAOa

[Tsu92b] Gene Tsudik. Message authentication with one-way hash functions. *Computer Communications Review, ACM SIGCOMM*, 22(5): 29–38, October 1992. CODEN CCRED2. ISSN 0146-4833.

Tsujii:1992:CS

[Tsu92c] Shigeo Tsujii. *Cryptography and security*, volume 1(2) of *Japanese technology reviews. Section B, Computers and communications*. Gordon and Breach, Langhorne, PA, USA, 1992. ISBN 2-88124-869-1. ISSN 1058-7306. xi + 156 pp. LCCN QA76.9.A25 T78 1992.

Thomlinson:1998:NBP

[TSY98] Matthew W. Thomlinson, Daniel R. Simon, and Bennet Yee. Non-biased pseudo random number generator. United States Patent 5,778,069., July 7, 1998. URL `http:www.google.com/patents/US5778069`.

Thersites:1984:IKE

[TT84a] Joan Thersites and John A. Thomas. An infinite key encryption system. *Dr. Dobb's Journal of Software Tools*, 9(8):44–??, August 1984. CODEN DDJOEB. ISSN 1044-789X.

Thomas:1984:IKE

[TT84b] John A. Thomas and Joan Thersites. Infinite key encryption system. *Dr. Dobb's Journal of Software Tools*, 9(8):44–??, August 1984. CODEN DDJOEB. ISSN 1044-789X.

Tiountchik:1999:RAF

[TT99] Alexander Tiountchik and Elena Trichina. RSA acceleration with field programmable gate arrays. *Lecture Notes in Computer Science*, 1587:164–176, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1587/15870164.htm; http://link.springer-ny.com/link/service/series/0558/papers/1587/15870164.pdf`.

Tual:1999:MGA

[Tua99] Jean-Pierre Tual. MASSC: a generic architecture for multiapplication smart cards. *IEEE Micro*, 19(5):52–61, September/October 1999. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL `http://dlib.computer.org/mi/books/mi1999/pdf/m5052.pdf; http://www.computer.org/micro/mi1999/m5052abs.htm`.

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 [Kah96b] describes this book as "recount[ing] the political effects of the most important cryptogram solution in history".

Tuckerman:1970:SVV

[Tuc70] Bryant Tuckerman. A study of the Vigenére–Vernam single and multiple loop enciphering systems. Research Report RC-2879, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, May 14, 1970.

Tuchman:1979:HPN

[Tuc79a] W. Tuchman. Hellman presents no shortcut solutions to DES. *IEEE Spectrum*, 16(7):40–41, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Tuchman:1979:IHP

[Tuc79b] W. Tuchman. IV. 'Hellman presents no shortcut solutions to the DES'. *IEEE Spectrum*, 16(7):40–41, July 1979. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Tung:1999:KNA

[Tun99] Brian Tung. *Kerberos: a Network Authentication System*. Addison-Wesley, Reading, MA, USA, 1999. ISBN 0-201-37924-4. 192 pp. LCCN TK5105.59.T86 1999. US$19.95.

Turing:1941:APC

[Tur41a] Alan M. Turing. The applications of probability to cryptography. Report, GCHQ, Cheltenham, UK, 1941. URL `http://www.gchq.gov.uk/Press/Pages/turing-papers-released.aspx`; `http://www.theregister.co.uk/2012/04/23/turing_papers_released/`. Unclassified and released 23 April 2012. Date uncertain, but believed to be between April 1941 and April 1942.

Turing:1941:SR

[Tur41b] Alan M. Turing. On statistics of repetitions. Report, GCHQ, Cheltenham, UK, 1941. URL `http://www.gchq.gov.uk/Press/Pages/turing-papers-released.aspx`; `http://www.theregister.co.uk/2012/04/23/turing_papers_released/`. Unclassified and released 23 April 2012. Date uncertain, but believed to be between April 1941 and April 1942.

Turing:1999:TTE

[Tur99] Alan Turing. Turing's treatise on Enigma. Technical report, CERN, Geneva, Switzerland, 1999. URL `http://home.cern.ch/~frode/crypto/Turing/index.html`. This document is retyped from the original (undated??) Turing typescript by the editors Ralph Erskine, Philip Marks and Frode

Weierud. Chapters 1, 2, and 6 (of 8) are available; the remainder are in preparation.

Tijdeman:1992:CDP

[Tv92] R. Tijdeman and Jacobus Henricus van Lint. *Cryptography and data protection: proceedings of a symposium at the Royal Netherlands Academy of Arts and Sciences on 19th December 1990*. Koninklijke Nederlandse Akademie van Wetenschappen, Verhandelingen, Afd. Natuurkunde. Eerste reeks; deel 38. North-Holland, Amsterdam, The Netherlands, 1992. ISBN 0-444-85746-X. vii + 104 pp. LCCN Q57 .A532.

Tel:1994:DAI

[TV94] Gerard Tel and Paul M. B. Vitanyi, editors. *Distributed algorithms: 8th international workshop / WDAG '94, Terschelling, the Netherlands, September 29–October 1, 1994, proceedings*, volume 857 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 3-540-58449-8 (Berlin), 0-387-58449-8 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.D5 I597 1994.

Tan:1992:NPE

[TX92] Yang Lin Tan and Dong Qing Xie. A note on probabilistic encryption. *Hunan Daxue Xuebao*, 19(3):20–25, 1992. CODEN HDAXE3. ISSN 1000-2472.

Takagi:1992:MMH

[TY92] N. Takagi and S. Yajima. Modular multiplication hardware algorithms with a redundant representation and their application to RSA cryptosystem. *IEEE Transactions on Computers*, 41(7):887–891, July 1992. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=256444.

Trabelsi:1994:PPS

[TY94] C. Trabelsi and A. Yongacoglu. Probability of packet success for asynchronous DS/CDMA with block and convolutional codes. *Lecture Notes in Computer Science*, 793:191–202, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tsiounis:1998:SEE

[TY98a] Y. Tsiounis and M. Yung. On the security of ElGamal-based encryption. *Lecture Notes in Computer Science*,

1431:117–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tsiounis:1998:SEB

[TY98b] Yiannis Tsiounis and Moti Yung. On the security of ElGamal-based encryption. *Lecture Notes in Computer Science*, 1431: 117–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310117.htm; http://link.springer-ny.com/link/service/series/0558/papers/1431/14310117.pdf.

Tax:1999:PFD

[TYD99] D. M. J. Tax, A. Ypma, and R. P. W. Duin. Pump failure detection using support vector data descriptions. *Lecture Notes in Computer Science*, 1642:415–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tygar:1996:CPI

[TYH96] J. D. Tygar, B. S. Yee, and N. Heintze. Cryptographic postage indicia. *Lecture Notes in Computer Science*, 1179:378–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tillich:1994:HS

[TZ94] Jean-Pierre Tillich and Gilles Zémor. Hashing with sl_2. In Desmedt [Des94b], pages 40–49. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390040.htm; http://link.springer-ny.com/link/service/series/0558/papers/0839/08390040.pdf.

Tzeng:1999:CMC

[Tze99] Wen-Guey Tzeng. Common modulus and chosen-message attacks on public-key schemes with linear recurrence relations. *Information Processing Letters*, 70 (3):153–156, May 14, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Udell:1998:HAW

[Ude98] Jon Udell. HTTP authentication — worried that anyone can get into your site? authentication is the answer, but not all Web servers do it the same. *BYTE Magazine*, 23(1):89–??, January 1998. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Uehara:1995:ESB

[Ueh95] Ryuhei Uehara. Efficient simulations by a biased coin. *Information Processing Letters*, 56(5):245–248, December 8, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Udell:1994:BCRb

[UFC94] Jon Udell, Rich Friedman, and Rick Cook. Books and CD-ROMs: PowerPC: Cultural and technological perspective: a chronicle of the PowerPC revolution, college selection via CD-ROM, and an encyclopedia of computer cracking via a network. *BYTE Magazine*, 19 (9):41–??, September 1994. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

USASC:1923:EC

[UG23] United States.Army.Signal Corps and George Fabyan Collection (Library of Congress). *Elements of cryptanalysis*. Number 3 in Training pamphlet. United States Government Printing Office, Washington, DC, USA, 1923. vii + 157 pp.

USWarDept:1924:EC

[Uni24a] United States.War Dept. *Elements of cryptanalysis*, volume 3 of *Its training pamphlet*. Government Printing Office, Washington, DC, USA, 1924. vii + 157 pp. LCCN Z104 .U6.

USWD:1924:EC

[Uni24b] United States.War Dept. *Elements of cryptanalysis*. Number 3 in Its Training pamphlet. United States Government Printing Office, Washington, DC, USA, 1924. vii + 157 pp.

USASC:1940:CML

[Uni40] United States Army Signal Corps. *Cryptanalyst's manual*. United States Government Printing Office, Washington, DC, USA, 1940. ???? pp. LCCN Z104 .U33c.

USASC:1942:ACC

[Uni42] United States.Army.Signal Corps. *Articles on cryptography and cryptanalysis*. United States Government Printing Office, Washington, DC, USA, 1942. v + 316 pp.

USDOS:1970:BC

[Uni70] United States.Dept.of the Army. *Basic cryptanalysis*. United States Government Printing Office, Washington, DC, USA, September 13, 1970. various pp.

USNBS:1977:DES

[Uni77] United States.National Bureau of Standards. *Data Encryption Standard*, volume 46 of *Federal Infor-*

mation Processing Standards publication. U.S. National Bureau of Standards, Gaithersburg, MD, USA, 1977. 18 pp. LCCN JK468.A8 A31 no.46.

USCSC:1978:CSD

[Uni78a] United States.Civil Service Commission. *Computer security and the Data Encryption Standard: proceedings of the Conference on Computer Security and the Data Encryption Standard held at the National Bureau of Standards in Gaithersburg, Maryland, on February 15, 1977*. Washington, DC, USA, 1978. viii + 125 pp.

USCSSC:1978:USN

[Uni78b] United States.Congress.Senate.Select Committee on Intelligence. *Unclassified summary — involvement of NSA in the development of the Data Encryption Standard: staff report of the Senate Select Committee on Intelligence, United States Senate*. United States Government Printing Office, Washington, DC, USA, April 1978. ii + 4 pp.

USNA:1979:CS

[Uni79a] United States.National Archives and Records Service. Cryptology studies. Records of the National Security Agency RG457, National Archives of the United States, Washington, DC, USA, 1979. ?? pp.

USNSG:1979:IRW

[Uni79b] United States.Naval Security Group. *Intelligence reports on the war in the Atlantic, 1942–1945: the account of the war in the Atlantic from Dec. 1942 to May 1945 as seen through and influenced by decryption of German naval radio traffic: [guide]*. Michael Glazier, Wilmington, DE, USA, 1979. 6 pp.

USNBS:1981:GIU

[Uni81] United States.National Bureau of Standards. *Guidelines for implementing and using the NBS Data Encryption Standard: category: ADP operations, subcategory: computer security*. FIPS Pub; 74. U.S. National Bureau of Standards, Gaithersburg, MD, USA, April 1, 1981. CODEN FIPPAT. 39 pp.

USDA:1982:SMM

[Uni82a] United States.Dept.of the Army. *Soldier's manual: MOS 32G: fixed cryptographic equipment repairer, skill levels 1 and 2*. Dept. of the Army, Headquarters, Washington, DC, USA (??), May 1982. various pp.

USDA:1982:TGM

[Uni82b] United States.Dept.of the

Army. *Trainer's guide: MOS 32G: fixed cryptographic equipment repairer*. Dept. of the Army, Headquarters, Washington, DC, USA (??), May 14, 1982. 35 pp.

USGSA:1982:TGS

[Uni82c] United States.General Services Administration. *Telecommunications: general security requirements for equipment using the Data Encryption Standard*. General Services Administration, Washington, DC, USA, April 14, 1982. 12 pp. Federal Standard 1027.

USNBS:1983:FPD

[Uni83] *FIPS Pub 46: Data Encryption Standard. FIPS publication change notice*, page various, 1983. U.S. Department of Commerce, National Bureau of Standards, Washinton, DC, USA.

USGSAOIRM:1984:ISR

[Uni84] United States.General Services Administration.Office of Information Resources Management. *Interoperability and security requirements for use of the Data Encryption Standard in the physical layer of data communications*. Office of Information Resources Management, 1984. various pp. Cover title. "August 3, 1983." "FSC TELE.".

USGAOPEMD:1987:PDD

[Uni87] United States.General Accounting Office.Program Evaluation and Methodology Division. *Privacy data: the Data Encryption Standard provides valuable protection*. Transfer paper - Program Evaluation and Methodology Division; 8 Transfer paper (United States. General Accounting Office. Program Evaluation and Methodology Division); 8. The Division, Washington, DC, USA, 1987. 80 pp.

USDA:1988:CED

[Uni88a] United States.Dept.of the Army. Cryptographic equipment destroyer, incendiary, TH1/TH4, M1A1, M1A2, and M2A1: ammunition surveillance procedures. Department of the Army supply bulletin SB 742-1375-94-801, Dept. of the Army, Headquarters, Washington, DC, USA (??), April 6, 1988. various pp. Supersedes SB 742-1375-94-3, 21 March 1974.

USNBS:1988:DES

[Uni88b] United States.National Bureau of Standards. *Data Encryption Standard*. Number 46-1 in Federal Information Processing Standards publication. National Technical Information Service, Washington, DC, USA, 1988. 16 pp. LCCN JK468.A8

A31 no.46 1988. Category: ADP operations; subcategory: computer security. Supersedes FIPS PUB 46, 1977 January 15. Shipping list no.: 88-367-P. Reaffirmed 1988 January 22.

USNSACSSCCH:1992:FLT

[Uni92] United States.National Security Agency/Central Security Service.Center for Cryptologic History. *The Friedman legacy: a tribute to William and Elizebeth Friedman*, volume 3 of *United States cryptologic history. Sources in cryptologic history*. Center for Cryptologic History, Fort George G. Meade, MD, USA, 1992. v + 282 pp.

USDOA:1994:OMT

[Uni94a] United States.Dept.of the Army. *Operator's manual for trunk encryption devices KG-94 (NSN 5810-01-187-9909) and KG-194 (NSN 5810-01-283-1395)*. Headquarters, Dept. of the Army, Washington, DC, USA, 1994.

USDOA:1994:UDS

[Uni94b] United States.Dept.of the Army. *Unit and direct support maintenance manual for trunk encryption device KG-94 (NSN 5810-01-187-9909): KG-194 (NSN 5810-01-283-1395) ... HGF-94 (NSN 5810-01-083-2896)*. Headquarters, Dept. of the Army, Washington, DC, USA, April 1994. ?? pp. Supersedes TM 11-5810-361-23, 13 Sep 1990.

USNSACS:1994:SC

[Uni94c] United States.National Security Agency/Central Security Service.Center for Cryptologic History. *Sources on cryptology*. The Center, Fort George G. Meade, MD, USA, 1994. 59 pp.

USCSCJSTL:1995:ACC

[Uni95a] United States.Congress.Senate.Committee on the Judiciary.Subcommittee on Technology and the Law. The administration's Clipper chip key escrow encryption program: hearing before the Subcommittee on Technology and the Law of the Committee on the Judiciary, United States Senate, One Hundred Third Congress, second session ... May 3, 1994. Senate hearing; 103-1067 103-1067, United States Government Printing Office, Washington, DC, USA, 1995. ISBN 0-16-047780-8. iv + 155 pp.

USNSGC:1995:NDN

[Uni95b] United States.Naval Security Group Command. *A new direction for naval cryptology*. Naval Security Group Command, Washington, DC, USA, 1995. 12 pp. URL `http://`

www.fas.org/irp/agency/navsecgru/org.htm.

UCC:1996:SRP

[Uni96a] Uniform Code Council. Summary of researching a potential standard for high capacity data encryption technologies for UCC and VICS. Technical report, Uniform Code Council, Dayton, OH, USA, January 10, 1996. various pp.

USPTO:1996:CCP

[Uni96b] United States Patent and Trademark Office. *Class 380 Cryptography... Patent Classification Definitions... Patent And Trademark Office... U.S. Dept. of Commerce*, December 1996. Shipping List no.: 97-0714-M Shipping List Date: 07/21/97.

USCHCJ:1996:SFT

[Uni96c] United States.Congress.House.Committee on the Judiciary. *Security and Freedom through Encryption (SAFE) Act hearing before the Committee on the Judiciary, House of Representatives, One Hundred Fourth Congress, second session, on H.R. 3011 ... September 25, 1996*. United States Government Printing Office, Washington, DC, USA, 1996. ISBN 0-16-053944-7. iii + 102 pp. LCCN KF27.J8 104th. Serial no. 100 (United States. Congress. House. Committee on the Judiciary). Shipping list no.: 97-0109-P. Serial no. 100.

USCHCCSTTCP:1997:SFT

[Uni97a] United States.Congress.House.Committee on Commerce.Subcommittee on Telecommunications, Trade, and Consumer Protection. *The Security and Freedom through Encryption (SAFE) Act: hearing before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, House of Representatives, One Hundred Fifth Congress, first session, on H.R. 695, September 4, 1997*. Washington, DC, USA, 1997. iii + 121 pp. Shipping list no.: 98-0034-P. Serial no. 105-39.

USCHCJSCIP:1997:SFT

[Uni97b] 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 Fifth Congress, first session, on H.R. 695 ... March 20, 1997*. United States Government Printing Office, Washington, DC, USA, 1997. ISBN

0-16-055287-7. iv + 166 pp. LCCN KF27.J8 105th. Shipping list no.: 97-0329-P. Serial no. 9.

USCSCJ:1997:EKR

[Uni97c] United States.Congress.Senate.Committee on the Judiciary. *Encryption, key recovery, and privacy protection in the information age: hearing before the Committee on the Judiciary, United States Senate, One Hundred Fifth Congress, first session on S. 376 ... S. 909 ... July 9, 1997*. Washington, DC, USA, 1997. iv + 130 pp. Shipping list no.: 98-0114-P. Serial No. J-105-31.

USGAOOGC:1997:DCB

[Uni97d] United States.General Accounting Office.Office of the General Counsel. Department of Commerce, Bureau of Export Administration: encryption items transferred from the U.S. munitions list to the commerce control list. Report GAO/OGC-97-12B-275864, United States. General Accounting Office. Office of the General Counsel, P.O. Box 37050, Washington, DC 20013, USA, January 13, 1997. 2 + 3 pp.

USCHCIR:1998:HEI

[Uni98a] United States.Congress.House.Committee on International Relations. *105-1 Hearing: Encryption: Individual Right to Privacy vs. National Security, May 8, 1997*. Washington, DC, USA, 1998. Shipping List no.: 98-0208-P. Shipping List Date: 04/20/1998.

USCHCIR:1998:MHS

[Uni98b] United States.Congress.House.Committee on International Relations. *105-1 Markup: H.R. 695: Security and Freedom Through Encryption (SAFE) Act, June 24, 1997*. Washington, DC, USA, 1998. Shipping List no.: 98-0348-P. Shipping List Date: 08/28/1998.

USCHCIR:1998:HSF

[Uni98c] United States.Congress.House.Committee on International Relations. *H.R. 695, the Security and Freedom through Encryption (SAFE) Act: markup before the Committee on International Relations, House of Representatives, One Hundred Fifth Congress, first session, July 22, 1997*. United States Government Printing Office, Washington, DC, USA, 1998. ISBN 0-16-057295-9. iii + 59 pp. LCCN Y 4.IN 8/16:SE 2/4/997-2 Gov Pubs US Docs. Shipping list no.: 98-0348-P.

USCHCIRSIEPT:1998:EIR

[Uni98d] United States.Congress.House.Committee on International Relations.Subcommittee on International Economic Policy and Trade. *Encryption: individual right to privacy vs. national security: hearing before the Subcommittee on International Economic Policy and Trade of the Committee on International Relations, House of Representatives, One Hundred Fifth Congress, first session, May 8, 1997*. United States Government Printing Office, Washington, DC, USA, 1998. ISBN 0-16-056317-8. iii + 116 pp. LCCN KF27.I53 105th no.41. Shipping list no.: 98-0208-P.

USCHCIRSIEPT:1998:HSF

[Uni98e] United States.Congress.House.Committee on International Relations.Subcommittee on International Economic Policy and Trade. *H.R. 695, Security and Freedom through Encryption (SAFE) Act markup before the Subcommittees on International Economic Policy and Trade and Asia and the Pacific of the Committee on International Relations, House of Representatives, One Hundred Fifth Congress, first session, June 24, 1997*. United States Government Printing Office, Washington, DC, USA, 1998. ISBN 0-16-055991-X. iii + 25 pp. LCCN J61 .F71 105th no.20; KF27.I53 105th. Shipping list no.: 98-0120-P.

USCHCNS:1998:HSF

[Uni98f] United States.Congress.House.Committee on National Security. *H.R. 695, the Security and Freedom through Encryption Act: Committee on National Security, House of Representatives, One Hundred Fifth Congress, first session: hearing held July 30, 1997*. United States Government Printing Office, Washington, DC, USA, 1998. ISBN 0-16-056189-2. iii + 127 pp. LCCN J61 .A751 105th no.23. H.N.S.C. 105-23. Shipping List no.: 98-0171-P. Shipping List Date: 03/13/1998.

USCSCCST:1998:HEH

[Uni98g] United States.Congress.Senate.Committee on Commerce, Science, and Transportation. *105-1 Hearing: Encryption, Senate Hearing 105-322, March 19, 1997*. Washington, DC, USA, 1998. Shipping List no.: 98-0363-P. Shipping List Date: 09/11/1998.

USCSCCST:1998:EHB

[Uni98h] United States.Congress.Senate.Committee on Commerce, Science, and Transportation. *Encryption: hearing before the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Fifth*

Congress, first session, March 19, 1997, volume 105-322 of *Senate hearing*. United States Government Printing Office, Washington, DC, USA, 1998. ISBN 0-16-057387-4. v + 185 pp. LCCN J60 .I61 105th no.33. Shipping list no.: 98-0363-P.

USCSCJ:1998:HEK

[Uni98i] United States.Congress.Senate.Committee on the Judiciary. *105-1 Hearing: Encryption, Key Recovery, and Privacy Protection in the Information Age, Senate Hearing 105-263, July 9, 1997*. Washington, DC, USA, 1998. Shipping List no.: 98-0114-P. Shipping List Date: 01/27/1998.

USCSCJ:1998:HED

[Uni98j] United States.Congress.Senate.Committee on the Judiciary. *105-1 Hearing: The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry, S.Hrg. 105-415, September 3, 1997*. Washington, DC, USA, 1998. Shipping List no.: 98-0208-P. Shipping List Date: 04/20/1998.

USCSCJSTTGI:1998:EDC

[Uni98k] United States.Congress.Senate.Committee on the Judiciary.Subcommittee on Technology, Terrorism, and Government Information. *The encryption debate: criminals, terrorists, and the security needs of business and industry: hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary, United States Senate, One Hundred Fifth Congress, first session ... September 3, 1997*. Number 105-415 in Senate hearing. United States Government Printing Office, Washington, DC, USA, 1998. ISBN 0-16-056359-3. iv + 116 pp. LCCN J60 .J9 105th no.33; KF26.J8 105th. Shipping list no.: 98-0208-P. Serial no. J-105-43.

USNSACS:19xx:BPM

[Unixxa] United States.National Security Agency / Central Security Service.Center for Cryptologic History. The bombe: prelude to modern cryptanalysis. Technical report, Center for Cryptologic History, National Security Agency, Fort George G. Meade, MD, USA, 19xx. 6 pp.

USNSACS:19xx:PUC

[Unixxb] United States.National Security Agency / Central Security Service.Center for Cryptologic History. Pioneers in U.S. cryptology. Technical report, Center for Cryptologic History, Fort George G. Meade, MD, USA, 19xx. 23 pp.

USGSA:1983:ISR

[UNN83] United States.General Services Administration, National Communications System (U.S.). Office of Technology and Standards, and National Institute of Standards and Technology (U. S.). Interoperability and security requirements for use of the Data Encryption Standard in the physical layer of data communications. Technical report, General Services Administration, Office of Information Resources Management, Washington, DC, USA, August 3, 1983. 4 pp. Federal standard 1026. Federal information processing standards publication, FIPS PUB 139.

USGSA:1985:ISR

[UNN85] United States.General Services Administration, National Communications System (U.S.). Office of Technology and Standards, and National Institute of Standards and Technology (U. S.). Interoperability and security requirements for use of the Data Encryption Standard with CCITT group 3 facsimile equipment. Technical report, General Services Administration, Office of Information Resources Management, Washington, DC, USA, April 4, 1985. 2 pp. Federal standard 1028. Federal information processing standards publication, FIPS PUB 141.

USGSA:1994:TIR

[UNU94] United States.General Services Administration, National Communications System (U.S.). Office of Technology and Standards, and United States.General Services Administration.Office of Information Resources Management. Telecommunications: interoperability requirements for the encryption of meteor burst radio communications. Federal standard 1056, General Services Administration, Office of Information Resources Management, Washington, DC, USA, May 13, 1994. 5 pp. Shipping list no.: 94-0323-P.

USENIX:1988:USWa

[USE88a] USENIX, editor. *UNIX Security Workshop Proceedings, August 29–30, 1988. Portland, OR*. USENIX Association, Berkeley, CA, USA, 1988. LCCN QA76.8.U65 U55 1988(1)-1990(2)//.

USENIX:1988:PFU

[USE88b] USENIX Association, editor. *Proceedings of the (First) USENIX Security Workshop, August 29–30, 1988, Portland, OR, USA*. USENIX Association, Berkeley, CA, USA, 1988. LCCN QA76.8.U65 U55 1988(1)-1990(2)//.

USENIX:1988:UCPb

[USE88c] USENIX Association, editor. *USENIX Conference Proceedings (Dallas, TX, USA)*. USENIX Association, Berkeley, CA, USA, Winter 1988. ISBN ???? LCCN ????

USENIX:1989:UCPb

[USE89a] USENIX, editor. *USENIX Conference Proceedings, Summer, 1989. Baltimore, MD*. USENIX Association, Berkeley, CA, USA, Summer 1989.

USENIX:1989:PSU

[USE89b] USENIX Association, editor. *Proceedings of the Summer 1989 USENIX Conference: June 12 — June 16, 1989, Baltimore, Maryland USA*. USENIX Association, Berkeley, CA, USA, 1989. LCCN QA 76.76 O63 U83 1989.

USENIX:1990:USI

[USE90] USENIX Association, editor. *UNIX Security II: USENIX workshop proceedings, August 27–28, 1990, Portland, Oregon*. USENIX Association, Berkeley, CA, USA, 1990. LCCN QA 76.9 A25 U55 1990.

USENIX:1991:PWU

[USE91] USENIX Association, editor. *Proceedings of the Winter 1991 USENIX Conference: January 21-January 25, 1991, Dallas, TX, USA*. USENIX Association, Berkeley, CA, USA, 1991. LCCN QA 76.76 O63 U84 1992.

USENIX:1992:PWU

[USE92a] USENIX, editor. *Proceedings of the Winter 1992 USENIX Conference: January 20 — January 24, 1992, San Francisco, California*. USENIX Association, Berkeley, CA, USA, 1992.

USENIX:1992:USI

[USE92b] USENIX, editor. *UNIX Security III Symposium, September 14–17, 1992. Baltimore, MD*. USENIX Association, Berkeley, CA, USA, September 14–17, 1992. ISBN 1-880446-46-4. LCCN ????

USENIX:1993:USI

[USE93] USENIX Association, editor. *UNIX Security IV Symposium: October 4–6, 1993, Santa Clara, CA, USA*. USENIX Association, Berkeley, CA, USA, October 4–6, 1993. ISBN 1-880446-55-3. LCCN QA 76.9 A25 U54 1993.

USENIX:1994:PSU

[USE94] USENIX, editor. *Proceedings of the Summer 1994 USENIX Conference: June 6–10, 1994, Boston, Massachusetts, USA*. USENIX Association, Berkeley, CA, USA, 1994. ISBN 1-880446-62-6. LCCN QA 76.76 O63 U83 1994.

USENIX:1995:PUT

[USE95a] USENIX Association, editor. *Proceedings of the 1995 USENIX Technical Conference: January 16–20, 1995, New Orleans, Louisiana, USA*. USENIX Association, Berkeley, CA, USA, 1995. ISBN 1-880446-67-7. LCCN QA 76.76 O63 U88 1995.

USENIX:1995:PFUa

[USE95b] USENIX Association, editor. *Proceedings of the fifth USENIX UNIX Security Symposium: June 5–7, 1995, Salt Lake City, Utah, USA*. USENIX Association, Berkeley, CA, USA, 1995. ISBN 1-880446-70-7. LCCN QA76.8.U65 U55 1992(3)-1995(5).

USENIX:1995:PFUb

[USE95c] USENIX Association, editor. *Proceedings of the first USENIX Workshop of Electronic Commerce: July 11–12, 1995, New York, New York, USA*. USENIX Association, Berkeley, CA, USA, 1995. ISBN 1-880446-74-X. LCCN HF5548.33. U84 1995(1).

USENIX:1996:SAC

[USE96a] USENIX, editor. *10th Systems Administration Conference (LISA'96), September 29–October 4, 1996. Chicago, IL*. USENIX Association, Berkeley, CA, USA, 1996.

USENIX:1996:WEC

[USE96b] USENIX, editor. *2nd Workshop on Electronic Commerce, November 18–21, 1996. Oakland, CA*. USENIX Association, Berkeley, CA, USA, November 18–21, 1996.

USENIX:1996:CSW

[USE96c] USENIX, editor. *Computing Systems, Winter, 1996*. USENIX Association, Berkeley, CA, USA, Winter 1996.

USENIX:1996:PSUa

[USE96d] USENIX, editor. *Proceedings of the second USENIX Workshop on Electronic Commerce: November 18–21, 1996, Oakland, California*. USENIX Association, Berkeley, CA, USA, 1996. ISBN 1-880446-83-9. LCCN HF5004 .U74 1996. URL `http://www.usenix.org/publications/library/proceedings/ec96/index.html`.

USENIX:1996:PSA

[USE96e] USENIX, editor. *Proceedings of the sixth annual USENIX Security Symposium, focusing on applications of cryptography, July 22–25, 1996, San Jose, California*. USENIX Association, Berkeley, CA, USA, July 22–25, 1996. ISBN 1-880446-79-0. LCCN QA76.9.A25 U83 1996. URL http://www.usenix.org/publications/library/proceedings/sec96/.

USENIX:1996:PUA

[USE96f] USENIX, editor. *Proceedings of the USENIX 1996 annual technical conference: January 22–26, 1996, San Diego, California, USA*, USENIX Conference Proceedings 1996. USENIX Association, Berkeley, CA, USA, 1996. ISBN 1-880446-76-6. LCCN QA 76.76 O63 U88 1996.

USENIX:1996:USS

[USE96g] USENIX Association, editor. *6th USENIX Security Symposium, July 22–25, 1996. San Jose, CA*. USENIX Association, Berkeley, CA, USA, July 22–25, 1996.

USENIX:1998:PUWa

[USE98a] USENIX, editor. *Proceedings of the 2nd USENIX Windows NT Symposium: August 3–5, 1998, Seattle, Washington*. USENIX Association, Berkeley, CA, USA, 1998. ISBN 1-880446-95-2. LCCN QA76.76.O63 U885 1998. URL http://db.usenix.org/publications/library/proceedings/usenix-nt98.

USENIX:1998:PUWb

[USE98b] USENIX, editor. *Proceedings of the 3rd USENIX Workshop on Electronic Commerce: August 31–September 3, 1998, Boston, Mass*. USENIX Association, Berkeley, CA, USA, 1998. ISBN 1-880446-97-9. LCCN HF5004 .U74 1998. URL http://db.usenix.org/publications/library/proceedings/ec98.

USENIX:1998:PFT

[USE98c] USENIX, editor. *Proceedings of the FreeNIX Track: USENIX 1998 annual technical conference: June 15–19, 1998, New Orleans, LA*. USENIX Association, Berkeley, CA, USA, 1998. ISBN ???? LCCN ???? URL http://www.usenix.org/publications/library/proceedings/usenix98/freenix/.

USENIX:1998:SUS

[USE98d] USENIX, editor. *Seventh USENIX Security Symposium proceedings: conference proceedings: San Anto-*

nio, Texas, January 26–29, 1998. USENIX Association, Berkeley, CA, USA, 1998. ISBN 1-880446-92-8. LCCN QA76.9.A25 U83 1998. URL `http://db.usenix.org/publications/library/proceedings/sec98`.

USENIX:1999:PEU

[USE99a] USENIX, editor. *Proceedings of the eighth USENIX Security Symposium (Security '99), August 23–26, 1999, Washington, DC, USA*. USENIX Association, Berkeley, CA, USA, 1999. ISBN 1-880446-28-6. LCCN QA76.9.A25 U83 1999. URL `http://www.usenix.org/publications/library/proceedings/sec99/`.

USENIX:1999:PTSa

[USE99b] USENIX, editor. *Proceedings of the Thirteenth Systems Administration Conference (LISA XIII): November 7—12, 1999, Seattle, WA, USA*. USENIX Association, Berkeley, CA, USA, 1999. ISBN 1-880446-25-1. LCCN ???? URL `http://www.usenix.org/publications/library/proceedings/lisa99/`.

USENIX:1999:PUWa

[USE99c] USENIX, editor. *Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99): May 10–11, 1999, Chicago, Illinois, USA*. USENIX Association, Berkeley, CA, USA, 1999. ISBN 1-880446-34-0. LCCN TK7895.S62 U84 1999. URL `http://www.usenix.org/publications/library/proceedings/smartcard99/`.

USENIX:1999:UAT

[USE99d] USENIX, editor. *Usenix Annual Technical Conference. June 6–11, 1999. Monterey, California, USA*. USENIX Association, Berkeley, CA, USA, 1999. ISBN 1-880446-33-2. LCCN ???? URL `http://db.usenix.org/publications/library/proceedings/usenix99`.

USWD:1980:EC

[UU80] United States.War Dept and United States.Adjutant-General's Office. *Elements of cryptanalysis*. Training pamphlet; no. 3 War Dept document; no. 117 Training pamphlet (United States. War Dept.); no. 3. Document (United States. War Dept.); no. 117. United States Government Printing Office, Washington, DC, USA, 1980. 165 pp.

USWD:1983:EC

[UU83] United States.War Dept and United States.Adjutant-General's Office. *Elements of cryptanalysis*. United States. War Dept. Training pamphlet no. 3. War Dept document no. 117. United States Government Printing Office, Washington, DC, USA, 1983. 165 pp.

USDOA:1989:BC

[UU89] United States.Dept.of the Army and United States Army Intelligence School. *Basic cryptanalysis*. United States Army Intelligence School, Fort Devens, Ma., coordinating draft. edition, 1989. various pp.

USCHCJ:1997:SFT

[UU97a] United States.Congress.House.Committee on the Judiciary and United States.Congress.House.Committee on International Relations. Security and Freedom through Encryption (SAFE) Act: report together with additional view (to accompany H.R. 695) (including cost estimate of the Congressional Budget Office). Report 105-108, United States Government Printing Office, Washington, DC, USA, May 22, 1997. various pp.

USPBC:1997:AEC

[UU97b] United States.President Bill Clinton and United States.Congress.House.Committee on International Relations. Administration of export controls on encryption products: communication from the President of the United States transmitting revisions to the provisions that apply to the Department of Commerce in the Export Administration regulations, 15 CFR part 730 et seq.–received in the United States House of Representatives November 15, 1996, pursuant to 50 U.S.C. 1703(b). Technical Report 105-12, United States Government Printing Office, Washington, DC, USA, January 7, 1997. 5 pp.

VanderBank:1988:CFM

[VA88] Dirk Van der Bank and Edwin Anderssen. Cryptographic figures of merit. *Computers and Security*, 7(3):299–303, June 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404888900363.

Vadhri:1995:VID

[Vad95] Kumar S. Vadhri. VLSI implementation of the data encryption algorithm. Thesis (M.S.), Department of Electrical Engineering, University of Hawaii at Manoa, Manoa, HI, USA, 1995. x + 89 pp.

Valerio:1892:C

[Val92] Paul Louis Eugene Valerio. De la cryptographie. *Journal des Sciences militares, 9th series, Paris*, ??(??):??, December 1892.

Vamos:1985:BRB

[Vam85] T. Vamos. Book review: *Mr. Babbage's secret. The tale of a cypher — and APL*: Ole Immanuel Franksen. *Automatica*, 21(5):616, September 1985. CODEN ???? ISSN ???? URL http://www.sciencedirect.com/science/article/pii/0005109885900135.

VanTassel:1969:ACT

[Van69] Dennie Van Tassel. Advanced cryptographic techniques for computers. *Communications of the Association for Computing Machinery*, 12(12):664–665, December 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Vandeberg:1986:ICS

[Van86] Ronald D. Vandeberg. Implementation of a coprocessing system to support data encryption. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1986. 112 pp.

VanHeurck:1987:TNS

[Van87] Philippe Van Heurck. TRASEX: national security system for EFTs in Belgium. *Computer Networks and ISDN Systems*, 14(2–5):389–395, 1987. CODEN CNISE9. ISSN 0169-7552.

vanTilborg:1988:IC

[van88] Henk C. A. van Tilborg. *An introduction to cryptology*, volume SECS 52 of *The Kluwer international series in engineering and computer science; Communications and information theory*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1988. ISBN 0-89838-271-8. x + 170 pp. LCCN Z103 .T541 1988. US$45.00.

VanTilburg:1993:SKE

[Van93] J. Van Tilburg. Secret-key exchange with authentication. *Lecture Notes in Computer Science*, 741:71–86, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

VanOorschot:1995:DCS

[Van95a] P. C. Van Oorschot. Design choices and security implications in implementing Diffie–Hellman key agreement. *Lecture Notes in Computer Science*, 1025: 1–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

VanTilborg:1995:ACA

[Van95b] H. C. A. Van Tilborg. Authentication codes: an area where coding and cryptology meet. *Lecture Notes in Computer Science*, 1025: 169–??, 1995. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

vanRenesse:1996:OSC

[van96] Rudolf L. van Renesse, editor. *Optical security and counterfeit deterrence techniques: 1–2 February, 1996, San Jose, California*, volume 2659 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA, 1996. CODEN PSISDG. ISBN 0-8194-2033-6. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TS510.S63 v.2659.

vanDijk:1997:MIT

[van97a] Marten van Dijk. More information theoretical inequalities to be used in secret sharing? *Information Processing Letters*, 63 (1):41–44, July 30, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

vanRenesse:1997:ODS

[van97b] Rudolf L. van Renesse, editor. *Optical document security*. Artech House, Boston, MA, 1997. ISBN 0-89006-982-4. xxviii + 505 pp. LCCN HV6675.O67 1998. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1050.html`. Includes CD-ROM.

vanderLubbe:1998:BMC

[van98] J. C. A. (Jan C. A.) van der Lubbe. *Basic methods of cryptography*. Cambridge University Press, New York, NY, USA, 1998. ISBN 0-521-55559-0 (paperback), 0-521-55480-2 (hardback). xiv + 229 pp. LCCN QA76.9.A25 L83 1998.

Varaiya:1999:DSI

[Var99a] P. Varaiya. Design, simulation, and implementation of hybrid systems. *Lecture Notes in Computer Science*, 1639:1–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Varma:1999:IDD

[Var99b] A. Varma. ICARUS: Design and deployment of a case-based reasoning system for locomotive diagnostics. *Lecture Notes in Computer Science*, 1650:581–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:1993:FHI

[Vau93] S. Vaudenay. FFT-Hash-II is not yet collision-free. *Lecture Notes in Computer Science*, 740:587–593, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:1995:NMC

[Vau95] S. Vaudenay. On the need for multipermutations: cryptanalysis of MD4 and SAFER. In Preneel [Pre95a], pages 286–297. CODEN LNCSD9. ISBN 3-540-60590-8 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F37 1995.

Vaudenay:1996:WKB

[Vau96] S. Vaudenay. On the weak keys of Blowfish. *Lecture Notes in Computer Science*, 1039:27–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:1998:CCC

[Vau98a] S. Vaudenay. Cryptanalysis of the Chor–Rivest cryptosystem. *Lecture Notes in Computer Science*, 1462: 243–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:1998:PSB

[Vau98b] S. Vaudenay. Provable security for block ciphers by decorrelation. *Lecture Notes in Computer Science*, 1373: 249–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:1998:CCR

[Vau98c] Serge Vaudenay. Cryptanalysis of the Chor–Rivest cryptosystem. *Lecture Notes in Computer Science*, 1462:243–256, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620243.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620243.pdf`.

Vaudenay:1998:DFC

[Vau98d] Serge Vaudenay. Decorrelated fast cipher. In National Institute of Standards and Technology [Nat98], page 20. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf1/dfc-slides.pdf`. Only the slides for the conference talk are available.

Vaudenay:1998:FSE

[Vau98e] Serge Vaudenay, editor. *Fast software encryption: 5th international workshop, FSE '98, Paris, France, March 23–25, 1998: proceedings*, volume 1372 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. CODEN LNCSD9. ISBN 3-540-

64265-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25F77 1998.

Vaudenay:1999:FCD

[Vau99a] S. Vaudenay. Feistel ciphers with $L2$-decorrelation. *Lecture Notes in Computer Science*, 1556:1–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:1999:SC

[Vau99b] S. Vaudenay. On the security of CS-cipher. In Knudsen [Knu99c], pages 260–274. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Vaudenay:1999:SCC

[Vau99c] S. Vaudenay. On the security of CS-cipher. *Lecture Notes in Computer Science*, 1636:260–274, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:1999:RAC

[Vau99d] Serge Vaudenay. Report on the AES candidates. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm; http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available.

Vaden:1996:ETU

[VB96] Michael K. Vaden and Edward F. Bruner. Encryption technology and U.S. national security. CRS report for Congress 96-670 F, Congressional Research Service, The Library of Congress, Washington, DC, USA, August 8, 1996. 9 pp.

Viswanathan:1999:PVK

[VBD99] Kapali Viswanathan, Colin Boyd, and Ed Dawson. Publicly verifiable key escrow with limited time span. *Lecture Notes in Computer Science*, 1587:36–50, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1587/15870036.htm; http://link.springer-ny.com/link/service/series/0558/papers/1587/15870036.pdf.

Vally:1999:CRC

[VC99] J.-D. Vally and R. Courdier. A conceptual "role-centered" model for design of multi-agent systems. *Lecture Notes in Computer Science*, 1599:33–46, 1999. CODEN LNCSD9. ISSN

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

Vandewalle:1990:ECC

[VCF+90] Joos Vandewalle, David Chaum, Walter Fumy, Cees J. A. Jansen, Peter Landrock, and G. Roelofsen. A European call for cryptographic algorithms: RIPE: Race Integrity Primitives Evaluation. *Lecture Notes in Computer Science*, 434: 267–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340267.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340267.pdf.

Dijk:1995:LCP

[vD95a] Marten van Dijk. A linear construction of perfect secret sharing schemes. *Lecture Notes in Computer Science*, 950:23–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500023.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500023.pdf.

vanDijk:1995:LCP

[vD95b] Marten van Dijk. A linear construction of perfect secret sharing schemes. *Lecture Notes in Computer Science*, 950:23–34, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500023.htm; http://link.springer-ny.com/link/service/series/0558/papers/0950/09500023.pdf.

Dijk:1997:SCB

[vD97] M. van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 43 (2):712–714, March 1997. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061820.html.

vandenAssem:1986:CPA

[vdAvE86] R. van den Assem and W. J. van Elk. A chosen-plaintext attack on the Microsoft BASIC protection. *Computers and Security*, 5(1):36–45, March 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404886901161.

Vandermeulen:1999:ADM

[VDDR99] F. Vandermeulen, P. Demeester, P. De Ceuleners, and J.-M. Reynders. Automated design of modular SNMP-CORBA gateways and their application for the development of an ADSL access network manager. *Lecture Notes in Computer Science*, 1597: 223–238, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lubbe:1998:BMC

[vdL98] J. C. A. (Jan C. A.) van der Lubbe. *Basic methods of cryptography*. Cambridge University Press, New York, NY, USA, 1998. ISBN 0-521-55480-2 (hardback), 0-521-55559-0 (paperback). xiv + 229 pp. LCCN QA76.9.A25 L8313 1998.

Wal:1997:PBR

[vdWS97] Ron van der Wal and William Stallings. Programmer's bookshelf — Ron examines Stanley Lippman's Inside the C++ Object Model, while William looks at Peter Wayner's Disappearing Cryptography. *Dr. Dobb's Journal of Software Tools*, 22(1):116–??, January 1997. CODEN DDJOEB. ISSN 1044-789X.

Vedder:1993:SAM

[Ved93] K. Vedder. Security aspects of mobile communications. *Lecture Notes in Computer Science*, 741:193–210, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vedder:1998:GSS

[Ved98a] K. Vedder. GSM: Security, services, and the SIM. *Lecture Notes in Computer Science*, 1528:224–240, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vedder:1998:ISI

[Ved98b] K. Vedder. International standardisation of IT security. *Lecture Notes in Computer Science*, 1528: 353–365, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Venema:1990:IEI

[Ven90] Terry Lee Venema. In-memory encryption and the impact on system security. Thesis (M.S.), Wright State University, Dayton, OH, USA, 1990. x + 90 pp.

Venkaiah:1992:RBP

[Ven92] V. Ch. Venkaiah. An RSA based public-key cryptosystem for secure communication. *Proc. Indian Acad. Sci. Math. Sci.*, 102(2):147–153, 1992. ISSN 0253-4142.

Vernam:1926:CPT

[Ver26] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal American Institute of Electrical Engineers*, XLV(??):109–115, 1926.

Veron:1995:CHI

[Ver95] P. Veron. Cryptanalysis of Harari's identification scheme. *Lecture Notes in Computer Science*, 1025: 264–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Verschuren:1998:SCN

[Ver98a] J. Verschuren. Security of computer networks. *Lecture Notes in Computer Science*, 1528:163–185, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Verschuren:1998:SAS

[Ver98b] Ton Verschuren. Smart access: strong authentication on the web. *Computer Networks and ISDN Systems*, 30(16–18):1511–1519, September 30, 1998. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic). URL `http://www.elsevier.com/cas/tree/store/comnet/sub/1998/30/16-18/2009.pdf`.

VonzurGathen:1999:MCA

[VG99] Joachim Von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, New York, NY, USA, 1999. ISBN 0-521-64176-4. xiii + 753 pp. LCCN QA76.9.A43 Z87 1999. US$59.95. Chapters 1 and 21 cover cryptography and public key cryptography.

Vandewalle:1993:TAT

[VGP93] J. Vandewalle, R. Govaerts, and B. Preneel. Technical approaches to thwart computer fraud. *Lecture Notes in Computer Science*, 741:20–32, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vallee:1988:HBO

[VGT88] Brigitte Vallée, Marc Girault, and Philippe Toffin. How to break Okamoto's cryptosystem by reducing lattice bases. *Lecture Notes in Computer Science*, 330: 281–291, 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vallee:1989:HGR

[VGT89] Brigitte Vallée, Marc Girault, and Philippe Toffin. How to guess l th roots modulo n by reducing lattice bases. In Mora [Mor89], pages 427–442. CODEN LNCSD9. ISBN 0-387-51083-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .A35 1988. US$36.00 (USA).

Verschuren:1993:IOS

[VGV93] J. Verschuren, R. Govaerts, and J. Vandewalle. ISO-OSI security architecture. *Lecture Notes in Computer Science*, 741:179–192, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

vanFaber:1997:SDD

[vHH97] E. van Faber, R. Hammelrath, and F. P. Heider. The secure distribution of digital contents. In IEEE [IEE97b], pages 16–22. ISBN 0-8186-8274-4 (paperback), 0-8186-8275-2 (casebound), 0-8186-8276-0 (microfiche). LCCN QA76.9.A25 C6375 1997. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064191.html`. IEEE Computer Society Press order number PR08274. IEEE order plan catalog number 97TB100213.

vanHeijst:1993:NCF

[vHPP93] Eugène van Heijst, Torben Pryds Pedersen, and Birgit Pfitzmann. New constructions of fail-stop signatures and lower bounds (extended abstract). *Lecture Notes in Computer Science*, 740:15–30, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0740/07400015.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0740/07400015.pdf`.

Vigna:1998:CTM

[Vig98] G. Vigna. Cryptographic traces for mobile agents. *Lecture Notes in Computer Science*, 1419:137–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vincent:1971:PAG

[Vin71] C. H. Vincent. Precautions for accuracy in the generation of truly random binary numbers. *Journal of Physics. E: Scientific Instruments*, 4(11):825–828, 1971. CODEN JPSIAE. ISSN 0022-3735. URL `http://stacks.iop.org/0022-3735/4/i=11/a=007`. See corrigendum [Vin72].

Vincent:1972:CPA

[Vin72] C. H. Vincent. Corrigendum: Precautions for accuracy in the generation of truly random binary numbers. *Journal of Physics. E: Scientific Instruments*, 5(6):546, 1972. CODEN JPSIAE. ISSN 0022-3735.

URL http://stacks.iop.org/0022-3735/5/i=6/a=521. See [Vin71].

Vandenwauver:1998:SIE

[VJ98] M. Vandenwauver and F. Jorissen. Securing Internet electronic mail. *Lecture Notes in Computer Science*, 1528:209–223, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Voydock:1983:SMH

[VK83] Victor L. Voydock and Stephen T. Kent. Security mechanisms in high-level network protocols. *ACM Computing Surveys*, 15(2): 135–171, June 1983. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Voydock:1984:SMT

[VK84] Victor L. Voydock and Stephen T. Kent. Security mechanisms in a transport layer protocol. *Computer Networks: The International Journal of Distributed Informatique*, 8 (5–6):433–449, October/December 1984. CODEN CNETDP. ISSN 0376-5075.

VanRompay:1998:DCI

[VKR98] Bart Van Rompay, Lars R. Knudsen, and Vincent Rijmen. Differential cryptanalysis of the ICE encryption algorithm. *Lecture Notes in Computer Science*, 1372:270–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720270.htm; http://link.springer-ny.com/link/service/series/0558/papers/1372/13720270.pdf.

Lingen:1996:NDP

[vL96] D. van Lingen. The new Dutch passport. In van Renesse [van96], pages 67–73. CODEN PSISDG. ISBN 0-8194-2033-6. ISSN 0277-786X (print), 1996-756X (electronic). LCCN TS510.S63 v.2659. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1032.html.

Vigil:1996:MIS

[VM96] H. P. Vigil and M. Mueller. Making the Internet safe for e-commerce. *Datamation*, 42(16):64–65, October 1996. CODEN DTMNAT. ISSN 0011-6963.

Villasenor:1997:CCb

[VMS97a] J. Villasenor and W. H. Mangione-Smith. Configurable computing. *Scientific American [International Edition]*, 276(6):54–59, June 1997. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Villasenor:1997:CCa

[VMS97b] John Villasenor and William H. Mangione-Smith. Configurable computing. *Scientific American*, 276 (6):66–?? (Intl. ed. 54–59), June 1997. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/1997/0607issue/0697villasenor.html.

Kerckhoffs:1883:CMF

[vN83] Auguste Kerckhoffs (von Nieuwenhof). La cryptographie militaire. (French) [Military cryptography]. *Journal des Sciences Militaires*, IX(??):5–38, 161–191, January/February 1883. URL http://www.cl.cam.ac.uk/~fapp2/kerckhoffs/la_cryptographie_militaire_i.htm https://www.petitcolas.net/kerckhoffs/; https://www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf; https://www.petitcolas.net/kerckhoffs/crypto_militaire_2.pdf.

Varadharajan:1999:DER

[VNM99] Vijay Varadharajan, Khanh Quoc Nguyen, and Yi Mu. On the design of efficient RSA-based off-line electronic cash schemes. *Theoretical Computer Science*, 226 (1–2):173–184, September 17, 1999. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1999&volume=226&issue=1-2&aid=3232.

Voyatzis:1998:DWO

[VNP98] G. Voyatzis, N. Nikolaidis, and I. Pitas. Digital watermarking: an overview. In Theodoridis et al. [T+98], pages 9–12. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073181.html. Four volumes.

Venkataraman:1994:PAM

[VNW94] B. R. Venkataraman and R. E. Newman-Wolfe. Performance analysis of a method for high level prevention of traffic analysis using measurements from a campus network. In IEEE [IEE94c], pages 288–297. ISBN 0-8186-6795-8 (paperback), 0-8186-6796-6 (microfiche). LCCN QA76.9.A25 C6375. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/042183.html.

Venkataraman:1995:CEA

[VNW95] B. R. Venkataraman and R. E. Newman-Wolfe. Capacity estimation and auditability of network covert channels. In IEEE [IEE95b], pages 186–198. ISBN 0-7803-2540-0, 0-8186-7015-0, 0-7803-2541-9. LCCN QA 76.9 A25 I43 1995. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1018.html. IEEE Catalog Number 95CH35760.

Oorschot:1991:CPP

[vO91a] Paul C. van Oorschot. A comparison of practical public-key cryptosystems based on integer factorization and discrete logarithms. *Lecture Notes in Computer Science*, 537: 576–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370576.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370576.pdf.

vanOorschot:1991:CPP

[vO91b] Paul C. van Oorschot. A comparison of practical public key cryptosystems based on integer factorization and discrete logarithms. *Lecture Notes in Computer Science*, 537: 576–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370576.htm; http://link.springer-ny.com/link/service/series/0558/papers/0537/05370576.pdf.

vanOorschot:1992:CPP

[vO92] Paul C. van Oorschot. A comparison of practical public key cryptosystems based on integer factorization and discrete logarithms. In *Contemporary cryptology*, pages 289–322. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992.

Vogel:1985:LCC

[Vog85] Rainer Vogel. On the linear complexity of cascaded sequences. In Beth et al. [BCI85], pages 99–109. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0209.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=209. Held at the University of Paris, Sorbonne.

Volts:1941:BCP

[Vol41] James D. Volts. *Bibliography of cryptography:*

Part I: Cryptography. U. S. Army, Cincinnati, OH, USA, 1941. various pp. LCCN ???? Chronologically arranged, covering period 1518–1940, and indexed by authors.

VonZurGathen:1992:PEE

[Von92a] Joachim Von Zur Gathen. Processor-efficient exponentiation in finite fields. *Information Processing Letters*, 41(2):81–86, February 14, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

VonZurGathen:1992:PEF

[Von92b] Joachim Von Zur Gathen. Processor-efficient exponentiation in finite fields. *Information Processing Letters*, 41(2):81–86, February 14, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Voukalis:1980:DFC

[Vou80a] D. C. Voukalis. The distance factor in cryptosystems. *International Journal of Electronics Theoretical & Experimental*, 49(1):73–75, 1980. CODEN IJELA2. ISSN 0020-7217.

Voukalis:1980:GSE

[Vou80b] D. C. Voukalis. A good solution of the encryption problem using matrix code, distance factor and PN sequences. *Internat. J. Electron.*, 48(3):271–274, 1980. CODEN IJELA2. ISSN 0020-7217.

vanOorschot:1991:KPA

[vOW91] Paul C. van Oorschot and Michael J. Wiener. A known-plaintext attack on two-key triple encryption. In Damgård [Dam91a], pages 318–325. CODEN LNCSD9. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1990. DM69.00. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730318.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0473/04730318.pdf`.

vanOorschot:1996:DHK

[vOW96] Paul C. van Oorschot and Michael J. Wiener. On Diffie–Hellman key agreement with short exponents. In Maurer [Mau96b], pages 332–343. CODEN LNCSD9. ISBN 3-540-61186-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1996. URL `http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700332.htm`; `http://link.springer-`

ny.com/link/service/series/0558/papers/1070/10700332.pdf. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Voyatzis:1996:ATA

[VP96] G. Voyatzis and I. Pitas. Applications of toral automorphisms in image watermarking. In IEEE [IEE96e], pages 237–240. ISBN 0-7803-3258-X (softbound), 0-7803-3259-8 (casebound), 0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM). LCCN TK8315.I222 1996. Three volumes. IEEE catalog number 96CH35919.

Voyatzis:1998:DIW

[VP98] G. Voyatzis and I. Pitas. Digital image watermarking using mixing systems. *Computers and Graphics*, 22(4):405–416, July–August 1, 1998. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.elsevier.com/cas/tree/store/cag/sub/1998/22/4/564.pdf.

Voyatzis:1999:PDI

[VP99] George Voyatzis and Ioannis Pitas. Protecting digital-image copyrights: a framework. *IEEE Computer Graphics and Applications*, 19(1):18–24, January/February 1999. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic). URL http://computer.org/cga/cg1999/g1018abs.htm; http://dlib.computer.org/cg/books/cg1999/pdf/g1018.pdf.

Varadharajan:1997:ISP

[VPM97] Vijay Varadharajan, Josef Pieprzyk, and Yi Mu, editors. *Information security and privacy: second Australasian conference, ACISP'97, Sydney, NSW, Australia, July 7–9, 1997: proceedings*, volume 1270 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997. CODEN LNCSD9. ISBN 3-540-63232-8 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN A76.9.A25A279 1997.

Vassiliadis:1988:PEA

[VPS88] Stamatis Vassiliadis, Michael Putrino, and Eric M. Schwarz. Parallel encrypted array multipliers. *IBM Journal of Research and Development*, 32(4):536–551, July 1988. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Volts:1941:BC

[VS41] James D. Volts and David Shulman. *Bibliography of cryptography*. U. S. Army, Cincinnati, OH. USA, 1941. 93 pp. LCCN Z103.A1 V6 1941. Typewritten (carbon copy) Three heavy leaves precede sections II-IV (not included in pagination). This copy was made especially for the United States Army from the original manuscript. Third copy: pencilled note on cover. Contents: pt.1. Cryptography; pt.2. Titles relating indirectly to cryptography; pt.3. Rejected titles; pt.4. Author index.

vanderWal:1997:PBR

[vS97] Ron van der Wal and William Stallings. Programmer's bookshelf — Ron examines Stanley Lippman's Inside the C++ Object Model, while William looks at Peter Wayner's Disappearing Cryptography. *Dr. Dobb's Journal of Software Tools*, 22(1):116–??, January 1997. CODEN DDJOEB. ISSN 1044-789X.

VanEetvelt:1995:DPF

[VSB95] P. W. J. Van Eetvelt, S. J. Shepherd, and S. K. Barton. The distribution of peak factor in QPSK multi-carrier modulation. *Journal of Wireless Personal Communications*, 2(1/2):87–96, November 1995.

Varadharajan:1997:SSP

[VSH97] V. Varadharajan, R. Shankaran, and M. Hitchens. Security services and public key infrastructure for ATM networks. In IEEE Computer Society. Technical Committee on Computer Communications [IEE97l], pages 253–263. ISBN 0-8186-8141-1, 0-8186-8142-X (casebound), 0-8186-8143-8 (microfiche). ISSN 0742-1303. LCCN TK5105.5 .C82 1997. IEEE Computer Society Press order number PR08141. IEEE Order Plan number 97TB100179.

vanTilburg:1990:MPK

[vT90] Johan van Tilburg. On the McEliece public-key cryptosystem. *Lecture Notes in Computer Science*, 403: 119–131, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

vanTilburg:1993:TCP

[vT93] Johan van Tilburg. Two chosen-plaintext attacks on the Li-Wang joint authentication and encryption scheme. In *Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993)*, volume 673 of *Lecture Notes in Comput. Sci.*, pages 332–343. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993.

vanTilburg:1994:SAC

[vT94] Johan van Tilburg. *Security-analysis of a class of cryptosystems based on linear error-correcting codes.* Technische Universiteit Eindhoven, Eindhoven, The Netherlands, 1994. ISBN 90-72125-45-2. ii + 199 pp. Dissertation, Technische Universiteit Eindhoven, Eindhoven, 1994.

vanTilburg:1986:DBK

[vTB86] Johan van Tilburg and Dick E. Boekee. Divergence bounds on key equivocation and error probability in cryptanalysis. *Lecture Notes in Computer Science*, 218:489–513, 1986. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

vanSchyndel:1994:DW

[vTO94] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. A digital watermark. In Anonymous [Ano94e], pages 86–90. ISBN 0-8186-6951-9 (microfiche). LCCN TA 1637 I25 1994. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1044.html`. Three volumes. IEEE Computer Society Press Order Number 6950-02. IEEE catalog number 94CH35708.

Vu:1995:CPM

[Vu95] Nguyen Cao Vu. CipherTEXT: purpose and method of an encryption/decryption utility. Thesis (B.S.), California Polytechnic State University, San Luis Obispo, CA, USA, 1995. v + 20 pp.

Vazirani:1985:ESP

[VV85] Umesh V. Vazirani and Vijay V. Vazirani. Efficient and secure pseudo-random number generation (extended abstract). In Blakley and Chaum [BC85], pages 193–202. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=193`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Valiant:1986:NED

[VV86] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, ???? 1986. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Verheul:1997:CLS

[Vv97] Eric R. Verheul and Henk C. A. van Tilborg. Cryptanalysis of "less short" RSA secret exponents. *Applicable algebra in engineering, communication and computing*, 8(5):425–435, 1997. CODEN AAECEW. ISSN 0938-1279 (print), 1432-0622 (electronic).

Vandemeulebroecke:1990:SCB

[VVDJ90] André Vandemeulebroecke, Etienne Vanzieleghem, Tony Denayer, and Paul G. A. Jespers. A single chip 1024 bits RSA processor. *Lecture Notes in Computer Science*, 434:219–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340219.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340219.pdf.

Verheul:1997:BEF

[VvT97] Eric R. Verheul and Henk C. A. van Tilborg. Binding ElGamal: a fraud-detectable alternative to key-escrow proposals. *Lecture Notes in Computer Science*, 1233:119–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330119.htm; http://link.springer-ny.com/link/service/series/0558/papers/1233/12330119.pdf.

vanOorschot:1994:PCS

[vW94] P. C. van Oorschot and M. J. Wiener. Parallel collision search with applications to hash functions and discrete logarithms. In ACM [ACM94a], pages 210–218. ISBN 0-89791-732-4. LCCN QA 76.9 A25 A26 1994. URL http://www.acm.org/pubs/contents/proceedings/commsec/191177.

VanOorschot:1996:DKA

[VW96] P. C. Van Oorschot and M. J. Wiener. On Diffie–Hellman key agreement with short exponents. *Lecture Notes in Computer Science*, 1070:332–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vedder:1998:SCR

[VW98] K. Vedder and F. Weikmann. Smart cards — requirements, properties, and applications. *Lecture Notes in Computer Science*, 1528: 307–331, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

vanOorschot:1999:PCS

[vW99] Paul C. van Oorschot and Michael J. Wiener. Parallel collision search with cryptanalytic applications. *Journal of Cryptology*, 12 (1):1–28, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/bibs/12n1p1.html`; `http://link.springer.de/link/service/journals/00145/papers/12n1p1.pdf`; `http://link.springer.de/link/service/journals/00145/papers/12n1p1.tex`.

vanEmdeBoas:1999:ALP

[vWN99] P. van Emde Boas, J. Wiedermann, and M. Nielsen, editors. *Automata, languages and programming: 26th international colloquium, ICALP'99, Prague, Czech Republic, July 11–15, 1999: proceedings*, volume 1644 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66224-3. LCCN QA267 .I23 1999 Bar.

Vanstone:1997:ECC

[VZ97] Scott A. Vanstone and Robert J. Zuccherato. Elliptic curve cryptosystems using curves of smooth order over the ring Z_n. *IEEE Transactions on Information Theory*, 43(4):1231–1237, 1997. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Waber:1987:VEC

[Wab87] John James Waber. Voice encryption for cellular telephones. Thesis (M.S.), University of Colorado, Boulder, CO, USA, 1987. x + 124 pp.

Weidenbach:1999:SDS

[WABC99] C. Weidenbach, B. Afshordel, U. Brahm, and C. Cohrs. System description: Spass version 1.0.0. *Lecture Notes in Computer Science*, 1632:378–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wobber:1993:ATO

[WABL93] Edward Wobber, Martín Abadi, Michael Burrows, and Butler Lampson. Authentication in the Taos operating system. *Operating Systems Review*, 27(5): 256–269, December 1993.

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

Wobber:1994:ATO

[WABL94] Edward Wobber, Martín Abadi, Michael Burrows, and Butler Lampson. Authentication in the Taos operating system. *ACM Transactions on Computer Systems*, 12(1):3–32, February 1994. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tocs/1994-12-1/p3-wobber/`.

Wade:1993:SLV

[Wad93] Andrew E. Wade. Single logical view over enterprise-wide distributed databases. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 22(2):441–444, June 1993. CODEN SRECD8. ISBN 0-89791-592-5. ISSN 0163-5808 (print), 1943-5835 (electronic).

Wadsen:1998:CLI

[Wad98] Wayne Wadsen. *Cryptography and liberty: an international survey of encryption policy*. Global Internet Liberty Campaign, ????, February 1998. various pp. URL `http://www.gilc.org/`; `mailto:info@gilc.org`.

Wagner:1983:F

[Wag83] Neal R. Wagner. Fingerprinting. In IEEE [IEE83], pages 18–22. ISBN 0-8186-0467-0 (paperback), 0-8186-4467-2 (microfiche), 0-8186-8467-4 (hardcover). LCCN QA76.9.A25 S95 1983. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1030.html`.

Wagner:1998:DCK

[Wag98a] D. Wagner. Differential cryptanalysis of KHF. *Lecture Notes in Computer Science*, 1372:293–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wagner:1998:CSR

[Wag98b] David Wagner. Cryptanalysis of some recently-proposed multiple modes of operation. In Vaudenay [Vau98e], pages 254–269. CODEN LNCSD9. ISBN 3-540-64265-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25F77 1998. URL `http://www.cs.berkeley.edu/~daw/multmode-fse98.ps`.

Wagner:1999:BA

[Wag99a] D. Wagner. The boomerang attack. In Knudsen [Knu99c], pages 156–170. ISBN 3-540-66226-X (softcover). LCCN QA76.9.A25 F77 1999 Bar.

Wagner:1999:CFb

[Wag99b] David Wagner. Cryptanalysis of FROG. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm`; `http://csrc.nist.gov/encryption/aes/round1/conf2/agenda-final.pdf`; `http://www.nist.gov/aes`. No slides for the conference talk are available.

Wagstaff:1999:C

[Wag99c] Samuel S. Wagstaff, Jr. Cryptanalysis. In Atallah [Ata99], pages 42–1–42–14. ISBN 0-8493-2649-4. LCCN QA76.9.A43A43 1999.

Waidner:1990:USR

[Wai90] M. Waidner. Unconditional sender and recipient untraceability in spite of active attacks. In Quisquater and Vandewalle [QV90], page ?? CODEN LNCSD9. ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1989; QA267.A1 L43 no.434. DM98.00. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1024.html`.

Waite:1995:BRB

[Wai95] William M. Waite. Book review: *Building in Big Brother: The Cryptographic Policy Debate*, Lance J. Hoffman. *Operating Systems Review*, 29(3):2, July 1995. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Walden:1900:ADB

[Wal00] John William Henry Walden. *August, Duke of Braunschweig-Luneburg: The cryptomenytics and cryptography of Gustavus Selenus: in nine books: wherein is also contained a most clear elucidation of the Steganographia, a book at one time composed in magic and enigmatic form by Johannes Trithemius.* ????, ????, 1900. LCCN Z103 .A95 1900.

Wallace:1990:PRG

[Wal90] C. S. Wallace. Physically random generator. *Computer Systems Science and Engineering*, 5(2):82–88, April 1990. CODEN CSSEEI. ISSN 0267-6192.

Wallich:1994:WP

[Wal94] Paul Wallich. Wire pirates. *Scientific American*, 270(3):90–?? (Int. ed. 72–??), March 1994. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Walton:1995:IAS

[Wal95] Steve Walton. Image authentication for a slippery new age. *Dr. Dobb's Journal of Software Tools*, 20(4): 18–20, 22, 24, 26, 82, 84–87, April 1995. CODEN DDJOEB. ISSN 1044-789X.

Walther:1998:VBE

[Wal98] Ursula Walther. *Verschlüsselungssysteme auf Basis endlicher Geometrien. (German) [Cryptosystems on the basis of finite geometries]*. Ph.D thesis, Justus-Liebig-Universität Giessen, Giessen, Germany, 1998. iii + 151 pp.

Walker:1999:CCI

[Wal99a] Michael Walker, editor. *Cryptography and Coding: 7th IMA Conference, Cirencester, UK, December 20–22, 1999: Proceedings*, volume 1746 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. CODEN LNCSD9. ISBN 3-540-66887-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1746. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1746.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1746`.

Wallich:1999:HSM

[Wal99b] Paul Wallich. How to steal millions in chump change. *Scientific American*, 281(2): ??, August 1999. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL `http://www.sciam.com/1999/0899issue/0899cyber.html`. Describes an off-shore credit card fraud scheme that in late 1998 accounted for as much as 4% of Visa chargebacks, and stole as much as US$45M from bogus US$19.95 transactions.

Walter:1999:MTI

[Wal99c] C. D. Walter. Moduli for testing implementations of the RSA cryptosystem. In Koren and Kornerup [KK99b], pages 78–85. ISBN 0-7803-5609-8, 0-7695-0116-8, 0-7695-0118-4. ISSN 1063-6889. LCCN QA76.6 .S887 1999. URL `http://euler.ecs.umass.edu/paper/final/paper-130.pdf; http://euler.ecs.umass.edu/paper/final/paper-130.ps`. IEEE Computer Society Order Number PR00116. IEEE Order Plan Catalog Number 99CB36336.

Wen-Ai:1994:MTS

[WAMO94] Jackson Wen-Ai, Keith M. Martin, and Christine M.

O'Keefe. Multisecret threshold schemes. *Lecture Notes in Computer Science*, 773:126–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wang:1986:UEA

[Wan86] Yuedong Wang. *Using encryption for authentication in local area networks*. ????, ????, 1986. ?? pp.

Wang:1992:CDS

[Wan92a] Dacheng Wang. Cryptosystem and digital signature scheme based on error-correcting codes. Thesis (M.S.), Computer Science Telecommunications Program. University of Missouri-Kansas City, Kansas City, MO, USA, 1992. vii + 48 pp.

Wang:1992:DKT

[Wan92b] Xiao Yun Wang. A Diophantine-knapsack type public-key cryptosystem. *Shandong Daxue Xuebao Ziran Kexue Ban*, 27(1): 29–34, 1992. CODEN SDXKEU. ISSN 0559-7234.

Warren:1982:BTC

[War82] Alexander Z. Warren. *Basic-plus through cryptanalysis; an introduction to structured programming*. ????, ????, 1982. 100 pp. Privately printed.

Ward:1998:ASE

[War98] Warren Ward. Applying stream encryption. *C/C++ Users Journal*, 16(9):??, September 1998. CODEN CCUJEX. ISSN 1075-2838.

Watler:1989:VAC

[Wat89] Miguel Watler. VLSI architectures and circuits for RSA encryption. Thesis (M.Sc.), Queen's University, Ottawa, ON, Canada, 1989. 137 pp.

Watt:1991:IPI

[Wat91] Stephen M. Watt, editor. *ISSAC '91: proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, July 15–17, 1991, Bonn, Germany*. ACM Press, New York, NY 10036, USA, 1991. ISBN 0-89791-437-6. LCCN QA 76.95 I59 1991.

Watson:1999:DOC

[Wat99] P. Watson. The design of an ODMG compatible parallel object database server (invited talk). *Lecture Notes in Computer Science*, 1573: 593–622, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wayner:1991:TDL

[Way91] Peter Wayner. True data: a look at techniques for ensuring the authenticity of the data you send, receive, or store. *BYTE Magazine*, 16(9):122–124, 126, 128, September 1991. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Wayner:1993:CAS

[Way93a] P. C. Wayner. Content-addressable search engines and DES-like systems. *Lecture Notes in Computer Science*, 740:575–586, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wayner:1993:ECD

[Way93b] Peter Wayner. Encryption chip draws fire: a new encryption chip promises to protect your electronic messages, but there's a catch: a trapdoor lets the government eavesdrop. *BYTE Magazine*, 18(8):36–??, July 1993. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Wayner:1993:SER

[Way93c] Peter Wayner. Should encryption be regulated: U.S. law enforcers want to limit your use of data encryption. *BYTE Magazine*, 18(6): 129–??, May 1993. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Wayner:1995:PCL

[Way95] Peter Wayner. Picking the crypto locks — with today's hardware and a new technique called differential cryptanalysis. it's getting easier for data burglars to crack your safe. what can you do to keep them out? *BYTE Magazine*, 20 (10):77–??, October 1995. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Wayner:1996:DCB

[Way96a] Peter Wayner. *Disappearing Cryptography: Being and Nothingness on the Net*. AP Professional, Boston, MA, USA, 1996. ISBN 0-12-738671-8. xi + 295 pp. LCCN TK5105.59 .W39 1996. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1042.html`.

Wayner:1996:DLY

[Way96b] Peter Wayner. Don't lose your crypto keys. *BYTE Magazine*, 21(5):137–??, May 1996. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Wayner:1998:MJD

[Way98] Peter Wayner. Making Java development JSafe — RSA's cryptographic toolkit targets Java as the platform of choice for secured Internet applications. *BYTE Magazine*, 23(1):117, January 1998. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Willcox:1992:TCS

[WB92] D. A. Willcox and S. R. Bunch. A tool for covert storage channel analysis of the UNIX kernel. In NIST [NIS92], pages 697–706. LCCN QA76.9.A25 N38 1992. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/021148.html`. Two volumes.

Wagner:1994:PPR

[WB94] David A. Wagner and Steven M. Bellovin. A programmable plaintext recognizer. Technical report, AT&T Bell Laboratories, Murray Hill, NJ, 1994. URL `http://www.research.att.com/~smb/papers/recog.pdf; http://www.research.att.com/~smb/papers/recog.ps`.

Wolf:1995:ICR

[WB95] Thomas Wolf and Andreas Brand. Investigating DEs with CRACK and related programs. *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 29(2S (special issue)): 1–8, June 1995. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

Whittle:1999:SDC

[WBBL99] J. Whittle, A. Bundy, R. Boulton, and H. Lowe. System description: C0YNTHIA. *Lecture Notes in Computer Science*, 1632:388–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wallach:1997:ESA

[WBDF97] Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Extensible security architectures for Java. *Operating Systems Review*, 31(5):116–128, December 1997. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Wu:1998:CRP

[WBDY98] H. Wu, F. Bao, R. H. Deng, and Q.-Z Ye. Cryptanalysis of Rijmen-Preneel trapdoor cipher. *Lecture Notes in Computer Science*, 1514: 126–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wegman:1981:NHF

[WC81] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, June 1981. CODEN JCSSBM. ISSN 0022-0000.

Wynn:1997:CTS

[WC97] Bruce Alan Wynn and Michael Carpenter. Cryptography tools for the systems administrator. *Sys Admin: The Journal for UNIX Systems Administrators*, 6 (6):45, 47–49, 51, June 1997. CODEN SYADE7. ISSN 1061-2688.

Weeks:1995:CBW

[WCS95] J. D. Weeks, A. Cain, and B. Sanderson. CCI-based Web security: a design using PGP. In O'Reilly and Associates and Web Consortium (W3C) [OW95], pages 381–396. ISBN 1-56592-169-0. ISSN 1085-2301. LCCN TK5105.888 .I68 1995. US$39.95. URL http://www.ora.com/gnn/bus/ora/item/wj1.html. The World Wide Web Journal is a quarterly publication that provides timely, in-depth coverage of the issues, techniques, and research developments in the World Wide Web. The December issue contains the Conference Proceeding papers that were chosen for the 4th International World Wide Web conference in Boston, MA.

Worthington:1986:IDS

[WCWG86] T. K. Worthington, J. J. Chainer, J. D. Willford, and S. C. Gunderson. IBM dynamic signature verification. *Computers and Security*, 5(2):167–168, June 1986. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488690146X.

Wolfgang:1996:WDI

[WD96] R. B. Wolfgang and E. J. Delp. A watermark for digital images. In IEEE [IEE96e], pages 219–222. ISBN 0-7803-3258-X (softbound), 0-7803-3259-8 (casebound), 0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM). LCCN TK8315.I222 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1033.html. Three volumes. IEEE catalog number 96CH35919.

Wolfgang:1997:WTD

[WD97] R. B. Wolfgang and E. J. Delp. A watermarking technique for digital imagery: Further studies. In Arabnia and Ahmed [AA97], pages 279–287. ISBN 0-9648666-9-2. LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1034.html.

Weber:1998:SMD

[WD98] D. Weber and T. Denny. The solution of McCurley's discrete log challenge. *Lecture Notes in Computer Science*, 1462:458–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wang:1999:SCB

[WD99a] Y. Wang and Y. Desmedt. Secure communication in broadcast channels: The answer to Franklin and Wright's question. *Lecture Notes in Computer Science*, 1592:446–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wendling:1999:PRS

[WD99b] L. Wendling and J. Desachy. Pattern recognition of strong graphs based on possibilistic c-means and k-formulae matching. *Lecture Notes in Computer Science*, 1566:180–189, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Weber:1979:USD

[Web79] Ralph Edward Weber. *United States Diplomatic Codes and Ciphers, 1775–1938*. Precedent Publishing, Chicago, IL, USA, 1979. ISBN 0-913750-20-4. xviii + 633 pp. LCCN Z103 .W4. US$49.95.

Webb:1988:NPK

[Web88] W. A. Webb. A nonlinear public key cryptosystem. *Computers and Mathematics with Applications*, 15(2):81–84, 1988. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Weber:1993:MDC

[Web93] Ralph Edward Weber. *Masked dispatches: cryptograms and cryptology in American history, 1775–1900*, volume 1 of *United States cryptologic history. Series 1, Pre-World War I; v. 1.* Center for Cryptologic History, National Security Agency, Fort George G. Meade, MD, USA, 1993. ISBN ???? vi + 236 pp. LCCN Z103.4.U6 W43 1993.

Weber:1998:SWY

[Web98] A. Weber. See what you sign: Secure implementations of digital signatures. *Lecture Notes in Computer Science*, 1430:509–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Webb:1999:UAO

[Web99] Alison Webb. User authentication: Options in Oracle. *Network Security*, 1999(12): 10–14, December 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800872487.

Wedemeijer:1999:DFM

[Wed99] L. Wedemeijer. Design the flexibility, maintain the stability of conceptual schemas. *Lecture Notes in Computer Science*, 1626: 467–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wehde:1997:UGT

[Weh97] E. D. Wehde. US gets tough on encryption. *Network Security*, 1997(10):9–10, October 1997. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485897857352.

Wehde:1998:MBE

[Weh98] Ed Wehde. Moves to break encryption deadlock. *Network Security*, 1998(8):6–7, August 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485898800718.

Wehde:1999:MSE

[Weh99] Ed Wehde. Military strength encryption for consumers. *Network Security*, 1999(7):6–7, July 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485899900090.

Weingarten:1983:CCP

[Wei83] F. Weingarten. Controlling cryptographic publication. *Computers and Security*, 2(1):41–48, January 1983. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/0167404883900330.

Weiss:1988:BOP

[Wei88] Eric A. Weiss. Biographies: Oh, pioneers! *Annals of the History of Computing*, 10(4):348–361, October/December 1988. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1988/pdf/a4348.pdf; http://www.computer.org/annals/an1988/a4348abs.htm.

Weissman:1991:IRA

[Wei91a] Clark Weissman. Inside RISKS: a national debate on encryption exportability. *Communications of the Association for Computing Machinery*, 34(10): 162, October 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/

Abstracts/0001-0782/125294.html.

Weissman:1991:IRN

[Wei91b] Clark Weissman. Inside RISKS: a national debate on encryption exportability. *Communications of the Association for Computing Machinery*, 34(10): 162, October 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/125294.html.

Weierud:1994:SPB

[Wei94] Frode Weierud. *The Secrets in The Park*: a book review. *Cryptolog*, 15(1):2, 18, January 1994. ISSN 0740-7602.

Weierud:1998:C

[Wei98] Frode Weierud. Cryptology. World-Wide Web site, 1998. URL http://frode.home.cern.ch/frode/crypto/.

Weierud:1999:TJG

[Wei99] Frode Weierud. TIRPITZ and the Japanese–German Naval War Communication Agreement. *Cryptolog*, 20 (3):6, 10, Summer 1999. ISSN 0740-7602.

Wells:1980:ADB

[Wel80] David L. Wells. Achieving data base protection through the use of subkey encryption. Thesis (Doctor of Engineering), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1980. 131 pp.

Welchman:1982:HSS

[Wel82a] Gordon Welchman. *The Hut Six story: breaking the Enigma codes*. McGraw-Hill, New York, NY, USA, 1982. ISBN 0-07-069180-0. ix + 326 pp. LCCN D810.C88 W44.

Wells:1982:USE

[Wel82b] David L. Wells. The use of subkey encryption to counter traffic analysis in communications networks. Technical report CSE 8201, Department of Computer Science and Engineering, Southern Methodist University, Dallas, TX, USA, February 1982. 24 pp.

Welchman:1986:PBB

[Wel86] G. Welchman. From Polish Bomba to British Bombe. The birth of Ultra. *Intelligence and National Security*, 1(1):71–110, ???? 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Wells:1988:NAI

[Wel88a] Codie Wells. A note on "Protection Imperfect". *Operating Systems Review*, 22(4):35, October 1988. CODEN OSRED8. ISSN 0163-5980. See [Hog88].

Welsh:1988:CC

[Wel88b] Dominic Welsh. *Codes and cryptography*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1988. ISBN 0-19-853288-1 (hardcover), 0-19-853287-3 (paperback). ix + 257 pp. LCCN Z103 .W461 1988. UK£30.00, US$60.00 (hardcover), UK£15.00 (paperback).

Welsh:1989:CC

[Wel89] Dominic Welsh. *Codes and cryptography*. Oxford science publications. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1989. ISBN 0-19-853287-3 (paperback). ix + 257 pp. LCCN Z 103 W46 1989. Reprinted with corrections.

Wells:1995:DEC

[Wel95] Thomas Wesson Wells. Data encryption: choices and implications for government, industry and the individual. Thesis (M.S.), University of Colorado, Boulder, CO, USA, 1995. xi + 90 pp.

Welchman:1997:HSS

[Wel97] Gordon Welchman. *The Hut Six story: breaking the Enigma codes*. M and M Baldwin, Cleobury Mortimer, Shropshire, UK, 1997. ISBN 0-947712-34-8. xiv + 263 pp. LCCN D810.C88 W44 1997.

Wernsdorf:1993:OFG

[Wer93a] R. Wernsdorf. The one-round functions of the DES generate the alternating group. *Lecture Notes in Computer Science*, 658: 99–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wernsdorf:1993:ORF

[Wer93b] Ralph Wernsdorf. The one-round functions of the DES generate the alternating group. *Lecture Notes in Computer Science*, 658:99–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580099.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580099.pdf`.

Worley:1994:PST

[WF94] P. H. Worley and I. T. Foster. Parallel spectral transform shallow water model: a runtime-tunable parallel benchmark code. In IEEE [IEE94e], pages 207–214. ISBN 0-8186-5680-8, 0-8186-5681-6. LCCN QA76.5 .S244 1994. IEEE catalog number 94TH0637-9.

Wagner:1998:CF

[WFS98] D. Wagner, N. Ferguson, and B. Schneier. Cryptanalysis of Frog. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, August 17, 1998. URL `http://www.counterpane.com/frog.html`.

Wagner:1999:CFa

[WFS99] D. Wagner, N. Ferguson, and B. Schneier. Cryptanalysis of FROG. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, April 1999. URL `http://www.counterpane.com/frog.html`. Second AES Candidate Conference, April 1999, to appear.

Wilkes:1982:MRJ

[WG82] Maurice V. Wilkes and I. J. Good. Meetings in retrospect: J. G. Brainerd on the ENIAC; A Report on T. H. Flowers's Lecture on Colossus. *Annals of the History of Computing*, 4(1):53–59, January/March 1982. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1982/pdf/a1053.pdf`; `http://www.computer.org/annals/an1982/a1053abs.htm`.

Wescombe:1997:GBS

[WG97] Peter Wescombe and John Gallehawk. Geting back into SHARK: H. M. S. Petard and the George Cross. Technical report, Bletchley Park Trust, Bletchley Park, UK, 1997. ???? pp.

Williams:1999:ADQ

[WG99] C. P. Williams and A. G. Gray. Automated design of quantum circuits. *Lecture Notes in Computer Science*, 1509:113–125, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wheeler:1987:BE

[Whe87] David Wheeler. Block encryption. Technical report 120, Computer Laboratory, University of Cambridge, Cambridge, Cambridgeshire, UK, 1987. 4 pp.

Wheeler:1994:BDE

[Whe94] D. Wheeler. A bulk data encryption algorithm. *Lecture Notes in Computer Science*, 809:127–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Want:1992:ABL

[WHFG92] Roy Want, Andy Hopper, Veronica Falcao, and Jonathan Gibbons. The active badge location system.

ACM Transactions on Information Systems, 10(1): 91–102, January 1992. CODEN ATISET. ISSN 1046-8188. URL http://www.acm.org:80.

White:1990:CDP

[Whi90] S. R. White. Covert distributed processing with computer viruses. In Brassard [Bra90c], pages 616–619. CODEN LNCSD9. ISBN 0-387-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1026.html. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

White:1993:NMM

[Whi93] M. Walker White. New methods of matrix encryption: using matrix factorization. Senior honors thesis, Department of Mathematics and Computer Science, Dartmouth College., Dartmouth, NH, USA, 1993. ii + 55 + 1 + 9 pp.

Whiting:1999:TNR

[Whi99] Doug Whiting. Twofish: New results. In National Institute of Standards and Technology [Nat99b], page 17. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/Whiting.pdf. Only the slides for the conference talk are available.

Wang:1999:CTG

[WHL99] Chih-Hung Wang, Tzonelih Hwang, and Narn-Yih Lee. Comments on two group signatures. *Information Processing Letters*, 69(2): 95–97, January 29, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Watanabe:1999:SGR

[WI99] Y. Watanabe and H. Imai. Shared generation of random number with timestamp: How to cope with the leakage of the CA's secret. *Lecture Notes in Computer Science*, 1560: 290–305, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wichmann:1987:NAR

[Wic87] B. A. Wichmann. Note on Algorithm 121: RSA key calculation in Ada. *The Computer Journal*, 30 (3):276, June 1987. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_30/Issue_03/tiff/276.tif. See [Hun85].

Wichmann:1990:CMR

[Wic90] Peer Wichmann. Cryptanalysis of a modified rotor machine. *Lecture Notes in Computer Science*, 434: 395–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340395.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340395.pdf.

Wiedemann:1986:QC

[Wie87] D. Wiedemann. Quantum cryptography. *ACM SIGACT News*, 18(2): 48–51, September/March 1986–1987. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Wiener:1990:CSRb

[Wie90a] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553–558, 1990. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Wiener:1990:CSRa

[Wie90b] Michael J. Wiener. Cryptanalysis of short RSA secret exponents (abstract). *Lecture Notes in Computer Science*, 434:372–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340372.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340372.pdf.

Wiener:1994:EKS

[Wie94] M. J. Wiener. Efficient DES key search. Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994. ?? pp. URL ftp://ripem.msu.edu/pub/crypt/docs/des-key-search.ps. Manuscript of August 20, 1993. Presented at the Rump Session of Crypto '93.

Wiener:1996:EKS

[Wie96] Michael J. Wiener. Efficient DES key search. In William R. Stallings, editor, *Practical Cryptography for Data Internetworks*, pages 31–79. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN ???? LCCN ???? URL ftp://ripem.msu.edu/pub/crypt/docs/des-key-search.ps. Presented at the Rump session of CRYPTO'93. Reprinted in Practical Cryptography for Data Internetworks, W. Stallings.

Wiener:1997:EKS

[Wie97] Michael J. Wiener. Efficient DES key search: An update. *CryptoBytes*, 3(2): 6–8, Autumn 1997. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto3n2.pdf`.

Wiener:1998:EKS

[Wie98a] Michael J. Wiener. Efficient DES key search — an update. *CryptoBytes*, 3(2):6–8, 1998.

Wiener:1998:PCP

[Wie98b] Michael J. Wiener. Performance comparison of public-key cryptosystems. *CryptoBytes*, 4(1):1, 3–5, Summer 1998. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto4n1.pdf`.

Wiener:1999:ACC

[Wie99] Michael Wiener, editor. *Advances in cryptology — CRYPTO '99: 19th annual international cryptology conference, Santa Barbara, California, USA, August 15–19, 1999 proceedings*, volume 1666 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Wilkins:1641:MSS

[Wil41] John Wilkins. *Mercury, or the Secret and Swift Messenger*. ????, ????, 1641. ???? pp.

Wilkes:1968:TSCa

[Wil68a] M. V. (Maurice Vincent) Wilkes. *Time-sharing computer systems*, volume 5 of *Macdonald computer monographs*. Macdonald and Co., London, UK, 1968. ISBN 0-356-02426-1. vii + 102 pp. LCCN QA76.5 .W523 1968b.

Wilkes:1968:TSCb

[Wil68b] M. V. (Maurice Vincent) Wilkes. *Time-sharing computer systems*, volume 5 of *Computer monograph series*. American Elsevier Pub. Co., New York, NY, USA, 1968. 102 pp. LCCN QA76.5 .W523.

Wilkes:1972:TSC

[Wil72] M. V. (Maurice Vincent) Wilkes. *Time-sharing computer systems*, volume 5 of *Computer monographs*. Macdonald and Co., London, UK, second edition, 1972. ISBN 0-444-19583-1 (Elsevier). ix + 149 pp. LCCN QA76.5 .W523 1972.

Wilkes:1975:TSC

[Wil75] M. V. (Maurice Vincent) Wilkes. *Time-sharing com-*

puter systems. Computer monographs. Macdonald and Jane's, London, UK, third edition, 1975. ISBN 0-444-19525-4 (American Elsevier). ii + 166 pp. LCCN QA76.53 .W54 1975.

Williams:1980:MRP

[Wil80] H. C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, 26(6): 726–729, 1980. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Willett:1982:CON

[Wil82a] Michael Willett. Cryptography old and new. *Computers and Security*, 1(2):177–186, June 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900104`.

Willett:1982:TPK

[Wil82b] Michael Willett. A tutorial on public key cryptography. *Computers and Security*, 1(1):72–79, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404882900281`.

Williams:1982:CHP

[Wil82c] Hugh C. Williams. Computationally "hard" problems as a source for cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 11–39. Westview, Boulder, CO, 1982.

Willett:1983:TKS

[Wil83a] Michael Willett. Trapdoor knapsacks without superincreasing structure. *Information Processing Letters*, 17(1):7–11, July 19, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Williams:1983:PAP

[Wil83b] M. H. Williams. The problem of absolute privacy. *Information Processing Letters*, 17(3):169–171, October 5, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Williams:1985:SPK

[Wil85] H. C. Williams. Some public-key crypto-functions as intractable as factorization. In Blakley and Chaum [BC85], pages 66–70. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25

C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=66. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Williams:1986:PKE

[Wil86a] H. C. Williams. An M^3 public-key encryption scheme. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 358–368. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1986.

Williams:1986:ACC

[Wil86b] Hugh C. Williams, editor. *Advances in cryptology — CRYPTO '85: proceedings: August 18–22, 1985*, volume 218 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1986. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm; http://www.springerlink.com/content/978-0-387-16463-2; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=218.

Williams:1986:CTU

[Wil86c] John J. Williams. *Cryptanalysis techniques: the ultimate decryption manual*. Consumertronics Co., Alamogordo, NM, USA, 1986. 11 + 3 + 1 pp.

Wiles:1993:HBE

[Wil93a] Gary Scott Wiles. Hardware based encryption for the personal computer using the Data Encryption Standard. Thesis (M.S.), Department of Electrical Engineering, University of Colorado at Denver, Denver, CO, USA, 1993. xii + 82 pp.

Williams:1993:CPK

[Wil93b] David Alan Williams. Comparison of public key encryption, private key encryption and digital signature. Thesis (Master of Computer Science), Lamar University, Beaumont, TX, USA, 1993. viii + 86 pp.

Wilcox:1998:SBW

[Wil98a] Jennifer E. Wilcox. *Sharing the burden: women in cryptology during World War II*. Center for Cryptologic History, National Security Agency, Fort George G. Meade, MD, USA, 1998. 18 pp. LCCN UB251.U5 W54 1998. URL http://proquest.safaribooksonline.com/01120100014SI; http://proquest.safaribooksonline.com/640.

Williams:1998:C

[Wil98b] H. C. Williams. Crypto '85. *Lecture Notes in Computer Science*, 1440:49–54, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Winterbotham:1969:SP

[Win69] F. W. (Frederick William) Winterbotham. *Secret and personal*. Kimber, London, UK, 1969. ISBN 0-7183-0321-0. 192 pp. LCCN D810.S7 W48; D810.S7 W73.

Winterbotham:1974:US

[Win74a] F. W. (Frederick William) Winterbotham. *The Ultra secret*. Weidenfeld and Nicolson, London, UK, 1974. ISBN 0-297-76832-8. xiii + 199 pp. LCCN D810.C88 W56.

Winterbotham:1974:USF

[Win74b] F. W. (Frederick William) Winterbotham. *The Ultra secret: the first account of the most astounding cryptanalysis coup of World War II — how the British broke the German code and read most of the signals between Hitler and his generals throughout the war*. Harper & Row, New York, NY, USA, 1974. ISBN 0-06-014678-8. xiii + 199 pp. LCCN D810.C95 W73 1974.

Winterbotham:1975:US

[Win75] F. W. (Frederick William) Winterbotham. *The Ultra secret*. Dell, New York, NY, USA, 1975. ISBN ???? 286 pp. LCCN D810.C88 W56 1976.

Winterbotham:1978:NC

[Win78] F. W. (Frederick William) Winterbotham. *The Nazi connection*. Harper & Row, New York, NY, USA, 1978. ISBN 0-06-014686-9. 222 pp. LCCN D810.S8 .W538 1978.

Winternitz:1983:POW

[Win83] Robert S. Winternitz. Producing a one-way hash function from DES. In Chaum et al. [CRS83], pages 203–207. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982.

Winternitz:1984:SOH

[Win84] Robert S. Winternitz. Secure one-way hash function built from DES. *Proceedings of the Symposium on Security and Privacy*, pages 88–90, 1984. CODEN PSSPEO. ISBN 0-8186-0532-4. IEEE Service Cent. Piscataway, NJ, USA.

Winterbotham:1989:US

[Win89] F. W. (Frederick William) Winterbotham. *The Ultra spy*. Macmillan, London, UK, 1989. ISBN 0-333-51425-4. 258 + 8 pp. LCCN UB271.G72 W564 1989. US$12.95.

Winterbotham:1991:US

[Win91] F. W. (Frederick William) Winterbotham. *The Ultra spy*. Papermac, London, UK, 1991. ISBN 0-333-55881-2 (paperback). 258 + 8 pp. LCCN UB271.G72 W564 1991.

Winton:1993:UPH

[Win93] John Winton. *Ultra in the Pacific: how breaking Japanese codes & ciphers affected naval operations against Japan, 1941–45*. L. Cooper and Naval Institute Press, London, UK and Annapolis, MD, USA, 1993. ISBN 0-85052-277-3, 1-55750-856-9. 247 pp. LCCN D810.C88 W58 1993.

Winterbotham:1999:US

[Win99] F. W. (Frederick William) Winterbotham. *The Ultra secret*. Weidenfeld and Nicolson, London, UK, 1999. ISBN 0-297-64405-X. xiii + 199 pp. LCCN D810.C88 W56 1999.

Wired:1998:REC

[Wir98] Wired News Report. RSA encryption challenge met! Contains announcement of a prize for cracking DES. The prize was claimed 39 days later [Ele98, p. xi]., February 24, 1998. URL `http://www.distributed.net/`; `http://www.wired.com/news/news/technology/story/10544.html`.

Wedel:1996:FSA

[WK96] G. Wedel and V. Kessler. Formal semantics for authentication logics. *Lecture Notes in Computer Science*, 1146:219–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Watanabe:1997:SCR

[WK97] H. Watanabe and T. Kasami. A secure code for recipient watermarking against conspiracy attacks by all users. In Han et al. [HOQ97], pages 413–423. CODEN LNCSD9. ISBN 3-540-63696-X (softcover). ISSN

0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25I554 1997. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064193.html.

Wechsler:1997:AVB

[WKHG97] H. Wechsler, V. Kakkad, J. Huang, and S. Gutta. Automatic video-based person authentication using the RBF network. *Lecture Notes in Computer Science*, 1206:85–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Whiting:1999:FOK

[WKS+99] Doug Whiting, John Kelsey, Bruce Schneier, David Wagner, Niels Ferguson, and Chris Hall. Further observations on the key schedule of Twofish. Twofish Technical Report 4, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, March 16, 1999. URL http://www.counterpane.com/twofish-ks2.html.

Woo:1992:ARC

[WL92a] T. Y. C. Woo and S. S. Lam. 'authentication' revisited (correction and addendum to 'Authentication' for distributed systems, Jan. 92, 39–52). *Computer*, 25(3):10, March 1992. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Woo:1992:ADS

[WL92b] Thomas Y. C. Woo and Simon S. Lam. Authentication for distributed systems. *Computer*, 25(1):39–52, January 1992. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). See correction [WL92c].

Woo:1992:CAD

[WL92c] Thomas Y. C. Woo and Simon S. Lam. Correction: Authentication for distributed systems. *Computer*, 25(3):10, March 1992. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). See [WL92b].

Woo:1994:LAP

[WL94] Thomas Y. C. Woo and Simon S. Lam. A lesson on authentication protocol design. *Operating Systems Review*, 28(3):24–37, July 1994. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Wong:1999:DSF

[WL99] Chung Kei Wong and Simon S. Lam. Digital signatures for flows and multicasts. *IEEE/ACM Transactions on Networking*, 7(4):502–513, August 1999. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL http://www.acm.org/pubs/citations/journals/ton/1999-7-4/p502-wong/.

Walker:1996:CKR

[WLEB96] Stephen T. Walker, Steven B. Lipner, Carl M. Ellison, and David M. Balenson. Commercial key recovery. *Communications of the Association for Computing Machinery*, 39(3):41–47, March 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/227240.html; http://www.acm.org/pubs/toc/Abstracts/cacm/227240.html.

Wagner:1985:PKC

[WM85] Neal R. Wagner and Marianne R. Magyarik. A public-key cryptosystem based on the word problem. In Blakley and Chaum [BC85], pages 19–36. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=19. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Waldvogel:1993:PDD

[WM93] C. P. Waldvogel and J. L. Massey. The probability distribution of the Diffie–Hellman key. *Lecture Notes in Computer Science*, 718: 492–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wheeler:1994:TCN

[WN94] David Wheeler and R. M. Needham. Two cryptographic notes. Technical report 355, University of Cambridge Computer Laboratory, Cambridge, UK, December 1994. 3 + 3 pp. Contents: A large block DES-like algorithm – TEA: a tiny encryption algorithm.

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). See [Bar05] for a retrospective.

Wheeler:1998:CX

[WN98a] David J. Wheeler and Roger M. Needham. Correction to XTEA. Report, Cambridge University, Cambridge, UK, October 1998. URL `http://www.movable-type.co.uk/scripts/xxtea.pdf`. See also original TEA [WN95] and first extension XTEA [NW97].

Wright:1998:NTD

[WN98b] Rebecca N. Wright and Peter G. Neumann, editors. *Network threats: DIMCS workshop, December 2–4, 1996*, volume 38 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.* American Mathematical Society, Providence, RI, USA, 1998. ISBN 0-8218-0832-X. LCCN TK5105.5 .N4668 1998.

Woehr:1997:CRR

[Woe97] Jack Woehr. A conversation with Ron Rivest: How important is cryptography and computer security? *Dr. Dobb's Journal of Software Tools*, 22(10):18–20, 22, 24, October 1997. CODEN DDJOEB. ISSN 1044-789X.

Wolfe:1943:FCCa

[Wol43a] Jack Martin Wolfe. *A first course in cryptanalysis*. Brooklyn college press, Brooklyn, NY, USA, 1943. ?? pp. LCCN Z104 .W6 1943 v. 1-3 (1943). Reproduced from type-written copy. Lesson 11 (44 numb) inserted after v. 2.

Wolfe:1943:FCCb

[Wol43b] Jack Martin Wolfe. *A first course in cryptanalysis*. University Press, Ann Arbor, MI, USA, 1943. various pp. Three volumes.

Wolfe:1943:FCCc

[Wol43c] Jack Martin Wolfe. *A first course in cryptanalysis*. Brooklyn College Press, Brooklyn, NY, USA, 1943. various pp. Three volumes.

Wolfe:1970:SWC

[Wol70] James Raymond Wolfe. *Secret writing: the craft of the cryptographer*. McGraw-Hill, New York, NY, USA, 1970. 192 pp. LCCN 652.8 W. Explains the distinction between ciphers and codes and describes their past and present use in secret communications.

Wolfe:1983:FCC

[Wol83] Jack Martin Wolfe. *A first course in cryptanalysis [!]*. Brooklyn College Press, Brooklyn, 1983. various pp. Three volumes.

Wolfowicz:1993:SPR

[Wol93a] W. Wolfowicz, editor. *State and progress of research in cryptography: 3rd Symposium — February 1993, Rome*, PROCEEDINGS

OF THE SYMPOSIUM ON STATE AND PROGRESS OF RESEARCH IN CRYPTOGRAPHY 1993; 3rd. [], Rome; Fondazione Ugo Bordoni, 1993.

Wolfowicz:1993:SPS

[Wol93b] William Wolfowicz, editor. *SPRC 93: proceedings of the 3rd Symposium of State and Progress of Research in Cryptography, Rome, 15–16 February, 1993*. Fondazione Ugo Bordoni, Rome, Italy, 1993. LCCN ????

Wolf:1998:SSAb

[Wol98] S. Wolf. Strong security against active attacks in information-theoretic secret-key agreement. *Lecture Notes in Computer Science*, 1514:405–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wolf:1999:USC

[Wol99] S. Wolf. Unconditional security in cryptography. *Lecture Notes in Computer Science*, 1561:217–250, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wood:1982:FAC

[Woo82] Charles Cresson Wood. Future applications of cryptography. *Computers and Security*, 1(1):65–71, January 1982. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/016740488290027X.

Woolsey:1990:DDE

[Woo90] Matthew A. Woolsey. Digital data encryption techniques with application to computer software access authorization. Thesis (M.S.E.), University of Arkansas, Fayetteville, Fayetteville, AR, USA, May 1990. viii + 125 pp.

Worth:1975:CMA

[Wor75] Vivian I. Worth. Cryptology: mathematical applications. Thesis (M.S.), Central Missouri State University, Warrensburg, MO, USA, 1975. iv + 63 pp.

Wortmann:1987:BRB

[Wor87] J. C. Wortmann. Book review: *Mr. Babbage's secret: The tale of a Cypher — and APL*: Strandberg, Birkerød, (Denmark) 1984, 319 pages. *European Journal of Operational Research*, 29(2): 216, May 1987. CODEN EJORDT. ISSN 0377-2217 (print), 1872-6860 (electronic). URL http://www.sciencedirect.com/science/article/pii/0221787901184.

World:1996:NIT

[Wor96] Linda World. In the news: Intel and TI will enter 3D graphics market; NRC releases report on cryptography. *IEEE Computer Graphics and Applications*, 16(4):92, July 1996. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic).

Wotawa:1999:NDD

[Wot99] F. Wotawa. New directions in debugging hardware designs. *Lecture Notes in Computer Science*, 1611: 226–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Waidner:1990:DCD

[WP90] Michael Waidner and Birgit Pfitzmann. The dining cryptographers in the disco: Unconditional sender and recipient untraceability with computationally secure serviceability (abstract). *Lecture Notes in Computer Science*, 434: 690–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340690.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340690.pdf`.

Wrixon:1989:CCS

[Wri89] Fred B. Wrixon. *Codes, ciphers, and secret language*. Harrap, London, UK, 1989. ISBN 0-245-54880-7. 266 pp. LCCN Z103 .W77 1989b.

Wright:1994:IRV

[Wri94] Benjamin Wright. Inside RISKS: The verdict on plaintext signatures: They're legal. *Communications of the Association for Computing Machinery*, 37(10):122, October 1994. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/175203.html`.

Wright:1998:ECC

[Wri98a] Marie A. Wright. The elliptic curve cryptosystem: a synopsis. *Network Security*, 1998(10):14–17, October 1998. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485800876035`.

Wrixon:1998:CCO

[Wri98b] Fred B. Wrixon. *Codes, ciphers & other cryptic & clandestine communication: making and breaking secret messages from hieroglyphs to the Internet*. Black Dog & Leventhal Publishers, New York, NY, USA, 1998. ISBN 1-57912-040-7.

704 pp. LCCN Z103.3 .W75 1998.

Wright:1999:EAE

[Wri99] Marie A. Wright. The evolution of the Advanced Encryption Standard. *Network Security*, 1999(11):11–14, November 1999. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485800800045.

Williams:1979:SRC

[WS79] H. C. Williams and B. Schmid. Some remarks concerning the M.I.T. public-key cryptosystem. *BIT*, 19(4):525–538, December 1979. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=19&issue=4&spage=525.

Wagner:1996:ASPa

[WS96a] David Wagner and Bruce Schneier. Analysis of the SSL 3.0 protocol. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1996. URL http://www.counterpane.com/ssl.html. Also published in *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 29–40.

Wagner:1996:ASPb

[WS96b] David Wagner and Bruce Schneier. Analysis of the SSL 3.0 protocol. In USENIX [USE96d], pages 29–40. ISBN 1-880446-83-9. LCCN HF5004 .U74 1996. URL http://www.counterpane.com/ssl.html.

Wiese:1996:SSS

[WS96c] Jim Wiese and Ed Shems. *Spy science: 40 secret-sleuthing, code-cracking, spy-catching activities for kids.* John Wiley and Sons, Inc., New York, NY, USA, 1996. ISBN 0-585-29524-7 (electronic), 0-471-14620-X. viii + 120 pp. LCCN JF1525.I6 W48 1996. URL http://www.loc.gov/catdir/bios/wiley041/96007019.html; http://www.loc.gov/catdir/description/wiley032/96007019.html; http://www.loc.gov/catdir/toc/onix03/96007019.html; http://www.netLibrary.com/urlapi.asp?action=summary&v=1&bookid=26341.

Wagner:1997:ASP

[WS97] David Wagner and Bruce Schneier. Analysis of the SSL 3.0 protocol. Report, University of California, Berkeley, Berkeley, CA, USA, April 15, 1997.

12 pp. URL `http://www.schneier.com/paper-ssl-revised.pdf`.

Whiting:1998:ITI

[WS98] D. Whiting and B. Schneier. Improved Twofish implementations. Twofish technical report 3, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, December 2, 1998. ???? pp. URL `http://www.counterpane.com/twofish-speed.html`.

White:1999:CBA

[WS99] S. White and D. Sleeman. A constraint-based approach to the description of competence. *Lecture Notes in Computer Science*, 1621: 291–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wagner:1998:CO

[WSD+98] D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier. Cryptanalysis of ORYX. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, August 1998. URL `http://www.counterpane.com/oryx.html`. Fifth Annual Workshop on Selected Areas in Cryptography, Springer-Verlag, August 1998, to appear.

Wagner:1999:CO

[WSDK99] D. Wagner, L. Simpson, E. Dawson, and J. Kelsey. Cryptanalysis of ORYX. *Lecture Notes in Computer Science*, 1556:296–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Weatherford:1999:NGA

[WSFC99] Margaret Weatherford, Keri Schreiner, Jenny Ferrero, and Crystal Chweh. News: Guide for all seasons: Lancaster's wireless tourist information system; coins (and billions) back Malaysia's MSC; data encryption: I'd like to solve the puzzle!; click to end world hunger. *IEEE Concurrency*, 7(3):4–8, July/September 1999. CODEN IECMFX. ISSN 1092-3063 (print), 1558-0849 (electronic). URL `http://dlib.computer.org/pd/books/pd1999/pdf/p3004.pdf`.

Wagner:1997:CCMa

[WSK97a] David Wagner, Bruce Schneier, and John Kelsey. Cryptanalysis of the Cellular Message Encryption Algorithm. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, March

20, 1997. URL http://www.counterpane.com/cmea-abstract.html.

Wagner:1997:CCMb

[WSK97b] David Wagner, Bruce Schneier, and John Kelsey. Cryptanalysis of the Cellular Message Encryption Algorithm. *Lecture Notes in Computer Science*, 1294: 526–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940526.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940526.pdf; http://www.counterpane.com/cmea-abstract.html.

Webster:1986:DB

[WT86] A. F. Webster and Stafford E. Tavares. On the design of S-boxes. In Williams [Wil86b], pages 523–534. CODEN LNCSD9. ISBN 0-387-16463-4 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1985; QA267.A1 L43 no.218. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm; http://www.springerlink.com/content/978-0-387-16463-2; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=218.

Whitten:1999:WJC

[WT99] Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In USENIX [USE99a], pages 169–184. ISBN 1-880446-28-6. LCCN QA76.9.A25 U83 1999. URL http://db.usenix.org/publications/library/proceedings/sec99/whitten.html; http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf; http://www2.cs.cmu.edu/~alma/johnny.pdf. Reprinted in [CG05, pp. 679–702].

Weiss:1985:RCM

[WTE+85] Eric A. Weiss, Henry S. Tropp, Ralph Erskine, John A. N. Lee, Gwen Bell, and M. R. Williams. Reviews: The Computer Museum and J. Bernstein, Three Degrees Above Zero: Bell Labs in the Information Age and D. R. Hartree, Calculating Machines: Recent and Prospective Developments and Their Impact on Mathematical Physics, and, Calculating Instruments and Machines and W. Kozaczuk, Enigma: How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two and S. Levy, Hackers and A. Osborne and J. Dvorak, Hypergrowth: The Rise and Fall of Osborne Computer Corporation and E. W. Pugh, Memories that Shaped an Industry and capsule reviews. *Annals of the History of Computing*, 7(3):258–277, July/ September 1985. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1985/pdf/a3258.pdf; http://www.computer.org/annals/an1985/a3258abs.htm.

Wu:1992:GOC

[Wu92] Chih-Kuo Wu. Group oriented cryptosystem and digital signature scheme without the assistance of a mutually trusted party. Thesis (M.S.), Computer Science Telecommunications Program. University of Missouri-Kansas City, Kansas City, MO, USA, 1992. vii + 43 pp.

Wu:1996:SNL

[Wu96] S. F. Wu. Sleepy network-layer authentication service for IPSEC. *Lecture Notes in Computer Science*, 1146: 146–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Williams:1979:CAA

[WW79] P. W. Williams and D. Woodhead. Computer assisted analysis of cryptic crosswords. *The Computer Journal*, 22(1):67–70, February 1979. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Wah:1984:RAM

[WW84] P. K. S. Wah and M. Z. Wang. Realization and application of the Massey–Omura lock. In IEEE, editor, *1984 International Zurich Seminar on Digital Communications: applications of source coding, channel coding and secrecy coding: March 6–8, 1984, Zürich, Switzerland, Swiss Federal Institute of Technology: proceedings*, pages 175–182. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1984. LCCN TK7881.5 I65 1984. IEEE catalog number 84CH1998-4.

Westfeld:1998:SVC

[WW98a] Andreas Westfeld and Gritta Wolf. Steganography in a video conferencing system. *Lecture Notes in Computer Science*, 1525:32–47, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250032.htm; http://link.springer-ny.com/link/service/series/

0558/papers/1525/15250032.pdf.

Whiting:1998:EVT

[WW98b] D. Whiting and D. Wagner. Empirical verification of Twofish key uniqueness properties. Twofish technical report 2, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, September 22, 1998. ???? pp. URL `http://www.counterpane.com/twofish-keys.html`.

Wu:1995:DAC

[WWH95] Tzong-Chen Wu, Tzong-Sun Wu, and Wei-Hua He. Dynamic access control scheme based on the Chinese remainder theorem. *International Journal of Computer Systems Science and Engineering*, 10 (2):92–99, April 1995. CODEN CSSEEI. ISSN 0267-6192.

Wu:1993:CSB

[WY93] Tzong-Chen Wu and Yi-Shiung Yeh. Cryptosystem for selectively broadcasting separate secrets. *Computer Systems Science and Engineering*, 8(2):121–124, April 1993. CODEN CSSEEI. ISSN 0267-6192.

Wiener:1999:FAE

[WZ99] Michael J. Wiener and Robert J. Zuccherato. Faster attacks on elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 1556:190–200, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Xie:1998:BWB

[XA98] L. Xie and G. R. Arce. A blind wavelet based digital signature forimage authentication. In Theodoridis et al. [T+98], pages 21–24. ISBN 960-7620-05-4 (set), 960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN TK5102.9.E97 1998. URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073183.html`. Four volumes.

Xia:1997:MWD

[XBA97] Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce. Multiresolution watermark for digital images. In IEEE [IEE97h], pages 548–551. ISBN 0-8186-8183-7, 0-8186-8184-5 (case). LCCN TK8315 .I16 1997. Three volumes. IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144.

Xie:1992:PEC

[Xie92] Dong Qing Xie. Partially efficient computation and criteria of security for public key cryptosystems. *Hunan Daxue Xuebao*, 19(6):

50–56, 70, 1992. CODEN HDAXE3. ISSN 1000-2472.

Xie:1993:IPK

[Xie93] Dong Qing Xie. An investigation of public key cryptosystems of real polynomial type. *Hunan Daxue Xuebao*, 20(5):103–106, 1993. CODEN HDAXE3. ISSN 1000-2472.

Xie:1998:WDI

[Xie98] Liehua Xie. Watermarking digital image signatures for authentication. Thesis (M.E.E.), Dept. of Electric and Computer engineering, University of Delaware, Dover, DE, ???? 1998. xii + 88 pp. Principal faculty advisor: Gonzalo R. Arce.

Xu:1998:CEC

[XL98] Qiu Liang Xu and Da Xing Li. Constructing elliptic curves suitable for cryptosystems—methods and implementation. *Chinese Journal of Computers = Chi suan chi hsueh pao*, 21 (12):1059–1065, 1998. CODEN JIXUDT. ISSN 0254-4164.

Xu:1999:NTR

[XL99] Qiu Liang Xu and Da Xing Li. New threshold RSA cryptosystems. *Shandong Daxue Xuebao Ziran Kexue Ban*, 34(2):149–155, 1999. CODEN SDXKEU. ISSN 0559-7234.

Xiong:1999:LPK

[XLP99] Jin Tao Xiong, Hong Xiu Liu, and De Zhong Pi. The Lucas public-key cryptosystem and its security. *Dianzi Keji Daxue Xuebao*, 28 (4):397–401, 1999. CODEN DKDAEM. ISSN 1001-0548.

Xiao:1994:MMH

[XtTmW94] G. (Gozhen) Xiao, Tsung to Tai, and Yu min Wang, editors. *Mi ma hsueh chin chan = Chinacrypt'94: ti san chieh Chung-kuo mi ma hsueh hsueh shu hui i lun wen chi: 11–15 November 1994 at Xidian, China*. Ko hsueh chu pan she, Peiching, China, 1994. ISBN 7-03-004363-4. LCCN ????

Xu:1997:BPK

[XW97] Maozhi Xu and Efang Wang. A break of public key cryptosystem PKCY. *Science in China. Series E, Technological sciences*, 40 (4):396–404, 1997. CODEN SCETFO. ISSN 1006-9321 (print), 1862-281X (electronic).

Xu:1997:PCP

[XZZ97] Shouhuai Xu, Gendu Zhang, and Hong Zhu. On the properties of cryptographic protocols and the weaknesses of the BAN-like logics. *Operating Systems Review*, 31(4):12–23, October 1997. CODEN OS-

RED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Xu:1998:STP

[XZZ98] Shouhuai Xu, Gendu Zhang, and Hong Zhu. On the security of three-party cryptographic protocols. *Operating Systems Review*, 32 (3):7–20, July 1998. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic). See comments [Ng99].

Yacobi:1999:RMC

[Yac99a] Y. Yacobi. Risk management for E-cash systems with partial real-time audit. *Lecture Notes in Computer Science*, 1648:62–71, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yacobi:1999:RME

[Yac99b] Y. Yacobi. Risk management for E-cash systems with partial real-time audit. In Franklin [Fra99], pages 62–71. ISBN 3-540-66362-2 (softcover). LCCN HG1710 .F35 1999.

Yahalom:COMPSYS-7-4-451

[Yah94] Raphael Yahalom. Secure timeliness: On the cost of non-synchronized clocks. *Computing Systems*, 7(4): 451–465, Fall 1994. CODEN CMSYE2. ISSN 0895-6340.

Yamamura:1998:PCU

[Yam98a] A. Yamamura. Public-key cryptosystems using the modular group. *Lecture Notes in Computer Science*, 1431:203–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yamamura:1998:PKC

[Yam98b] Akihiro Yamamura. Public-key cryptosystems using the modular group. *Lecture Notes in Computer Science*, 1431:203–216, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310203.htm; http://link.springer-ny.com/link/service/series/0558/papers/1431/14310203.pdf`.

Yamamura:1999:FCU

[Yam99] A. Yamamura. A functional cryptosystem using a group action. *Lecture Notes in Computer Science*, 1587: 314–326, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yan:1995:PTL

[Yan95] S. Y. Yan. Primality testing of large numbers in Maple. *Computers and Mathematics with Applications*, 29

(12):1–8, June 1995. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Yao:1982:PSC

[Yao82a] A. Yao. Protocols for secure computation. In IEEE [IEE82a], pages 160–164. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

Yao:1982:TAT

[Yao82b] A. C. Yao. Theory and application of trapdoor functions. In IEEE [IEE82a], pages 80–91. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog no. 82CH1806-9. IEEE Computer Society order no. 440.

Yao:1986:HGE

[Yao86] A. C. Yao. How to generate and exchange secrets. In IEEE [IEE86b], pages 162–167. ISBN 0-8186-0740-8 (paperback), 0-8186-4740-X (microfiche), 0-8186-8740-1 (casebound). LCCN QA 76 S979 1986; TK7885.A1 S92 1986.

Yardley:1931:ABC

[Yar31] Herbert O. Yardley. *The American Black Chamber*. Faber & Faber Limited, London, UK, 1931. x + 264 + 1 pp. LCCN D639.S7 Y3 1931b. The history and work of the Cryptographic bureau, officially known as section 8 of the Military intelligence division (MI-8).

Yardley:1940:SSA

[Yar40] Herbert O. Yardley. *Secret service in America: The American Black Chamber*. Faber & Faber Limited, London, UK, 1940. x + 264 + 1 pp. LCCN D639.S7 Y3 1940. The history and work of the Cryptographic bureau, officially known as section 8 of the Military intelligence division (MI-8).

Yardley:1983:CBC

[Yar83] Herbert O. Yardley. *The Chinese Black Chamber: an adventure in espionage*. Houghton-Mifflin, Boston, MA, USA, 1983. ISBN 0-395-34648-7. xxiv + 225 pp. LCCN DS777.533.S65 Y37 1983. US$13.95. Chinese title: Chung-kuo hei shih.

Yardley:1990:ABC

[Yar90] Herbert O. Yardley. *The American Black Chamber*, volume 52 of *A cryptographic series*. Aegean Park Press, Laguna Hills, CA, USA, 1990. ISBN 0-89412-154-5 (paperback), 0-89412-155-3 (hard cover). 375 pp. LCCN D639.S7 Y3 1990. Originally published by Bobbs-Merrill, Indianapolis, IN, USA, 1931.

Yasaki:1976:EAK

[Yas76] E. K. Yasaki. Encryption algorithm: key size is the thing. *Datamation*, 22(3):164–166, March 1976. CODEN DTMNAT. ISSN 0011-6963.

Yoshiura:1998:VDW

[YEA+98] Hiroshi Yoshiura, Isao Echizen, Takao Arai, Hiroyuki Kimura, and Toshifumi Takeuchi. VSP: a digital watermark method for motion picture copyright protection. In IEEE [IEE98c], pages 338–339. CODEN DTPEEL. ISBN ???? ISSN 0747-668X. LCCN ???? IEEE catalog number 98CH36160.

Yeung:1997:DWH

[Yeu97] Minerva Ming-Yee Yeung. Digital watermarking for high-quality imaging. Research report RC 20797, IBM T.J. Watson Research Center, Yorktown Heights, NY, USA, 1997. 7 pp. To appear, IEEE First Workshop on Multimedia Signal Processing, Princeton NJ, Jun 23–25 '97.

Yeung:1998:DW

[Yeu98] Minerva M. Yeung. Digital watermarking. *Communications of the Association for Computing Machinery*, 41(7):30–33, July 1998. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/cacm/1998-41-7/p30-yeung/`.

Yeun:1999:DSM

[Yeu99] Chan Yeob Yeun. Digital signature with message recovery and authenticated encryption (signcryption)—a comparison. In *Cryptography and coding (Cirencester, 1999)*, volume 1746 of *Lecture Notes in Comput. Sci.*, pages 307–312. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999.

Yokokawa:1999:BDE

[YHKI99] M. Yokokawa, S. Habata, S. Kawai, and H. Ito. Basic design of the Earth simulator. *Lecture Notes in Computer Science*, 1615: 269–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yi:1996:DAN

[Yi96] X. Yi. On design and analysis of a new block cipher. *Lecture Notes in Computer Science*, 1179:213–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yin:1997:REA

[Yin97] Yiqun Lisa Yin. The RC5 encryption algorithm: Two years on. *CryptoBytes*, 2(3): 14–15, Winter 1997. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto2n3.pdf`.

Yakovlev:1998:PND

[YK98] A. V. Yakovlev and A. M. Koelmans. Petri nets and digital hardware design. *Lecture Notes in Computer Science*, 1491: 154–236, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yahalom:1994:TBN

[YKB94] Raphael Yahalom, Birgit Klein, and Thomas Beth. Trust-based navigation in distribution systems. *Computing Systems*, 7(1):45–73, Winter 1994. CODEN CMSYE2. ISSN 0895-6340.

Yang:1999:DIC

[YKY99] H. Yang, H. Kim, and J. Yang. Design and implementation of COIRS (a COncept-Based Image Retrieval System). *Lecture Notes in Computer Science*, 1614:391–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yen:1993:FCE

[YL93] S.-M. Yen and C.-S. Laih. The fast cascade exponentiation algorithm and its applications on cryptography. *Lecture Notes in Computer Science*, 718:447–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yen:1995:IDSb

[YL95a] S.-M. Yen and C.-S. Laih. Improved digital signature suitable for batch verification. *IEEE Transactions on Computers*, 44(7): 957–959, July 1995. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=392857`.

Yen:1995:IDSa

[YL95b] Sung-Ming Yen and Chi-Sung Laih. Improved digital signature algorithm. *IEEE Transactions on Computers*, 44(5):729–730, May 1995. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=381963`. See correction [Ano96f].

Yang:1997:NEC

[YL97a] Ching-Nung Yang and Chi-Sung Laih. A note on error-correcting codes for authentication and subliminal channels. *Information Processing Letters*, 62 (3):141–142 (or 141–143??), May 14, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/062621.html.

Yen:1997:SAT

[YL97b] Sung-Ming Yen and Kuo-Hong Liao. Shared authentication token secure against replay and weak key attacks. *Information Processing Letters*, 62(2):77–80, May 21, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Yi:1997:NHF

[YL97c] X. Yi and K.-Y. Lam. A new hash function based on block cipher. *Lecture Notes in Computer Science*, 1270:139–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yi:1998:NBB

[YLCY98a] X. Yi, Kwok Yan Lam, Shi Xin Cheng, and Xiao Hu You. A new byte-oriented block cipher. *Lecture Notes in Computer Science*, 1396: 209–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yi:1998:NBO

[YLCY98b] X. Yi, Kwok Yan Lam, Shi Xin Cheng, and Xiao Hu You. A new byte-oriented block cipher. *Lecture Notes in Computer Science*, 1396: 209–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ye:1999:CS

[YLD99] D.-F. Ye, K.-Y. Lam, and Z.-D. Dai. Cryptanalysis of "2R" schemes. In Wiener [Wie99], pages 315–325. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Yi:1998:DCB

[YLH98] Xun Yi, Kwok Yan Lam, and Yongfei Han. Differential cryptanalysis of a block cipher. *Lecture Notes in Computer Science*, 1438:58–67, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yeung:1998:IWI

[YM98] Minerva M. Yeung and Frederick C. Mintzer. Invisible watermarking for image verification. *Journal of Electronic Imaging*, 7(3): 578–591, July 1998. CODEN JEIME5. ISSN 1017-9909 (print), 1560-229X (electronic).

Yfoulis:1999:SOP

[YMWP99] C. A. Yfoulis, A. Muir, P. E. Wellstead, and N. B. O. L. Pettit. Stabilization of orthogonal piecewise linear systems: Robustness analysis and design. *Lecture Notes in Computer Science*, 1569:256–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

York:1996:BSN

[Yor96] Kyle A. York. Building a DOS serial network. *Dr. Dobb's Journal of Software Tools*, 21(5):38, 40–43, 80, May 1996. CODEN DDJOEB. ISSN 1044-789X.

Yourdon:1996:JWS

[You96] Edward Yourdon. Java, the Web, and software development. *Computer*, 29(8):25–30, August 1996. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Young:1997:IJA

[You97] Andrew Young. Implementation of JANET authentication and encryption services. Report 007, Joint Information Systems Committee (JISC) Technology Applications Programme, Manchester, UK, 1997. 21 pp.

Yeh:1991:EIC

[YS91] P. C. Yeh and R. M. Smith, Sr. ESA/390 integrated cryptographic facility: An overview. *IBM Systems Journal*, 30(2): 192–205, 1991. CODEN IBMSA7. ISSN 0018-8670.

Yeh:1999:CCC

[YS99] P. C. Yeh and R. M. Smith, Sr. S/390 CMOS cryptographic coprocessor architecture: Overview and design considerations. *IBM Journal of Research and Development*, 43(5/6):777–794, ???? 1999. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http://www.research.ibm.com/journal/rd/435/yeh.html`.

Yoshiura:1999:SFU

[YST99a] Hiroshi Yoshiura, Ryoichi Sasaki, and Kazuo Takaragi. Secure fingerprinting using public-key cryptography (position paper). *Lecture Notes in Computer Science*, 1550: 83–89, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1550/15500083.htm; http://link.springer-ny.com/link/service/series/0558/papers/1550/15500083.pdf`.

Yshiura:1999:SFU

[YST99b] H. Yshiura, R. Sasaki, and K. Takaragi. Secure fingerprinting using public-key cryptography. *Lecture Notes in Computer Science*, 1550:83–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Youssef:1995:RBB

[YT95a] A. M. Youssef and S. E. Tavares. Resistance of balanced *s*-boxes to linear and differential cryptanalysis. *Information Processing Letters*, 56(5):249–252, December 8, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Youssef:1995:RBS

[YT95b] A. M. Youssef and S. E. Tavares. Resistance of balanced *s*-boxes to linear and differential cryptanalysis. *Information Processing Letters*, 56(5):249–??, ???? ??, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Youssef:1996:CBN

[YT96] A. M. Youssef and S. E. Tavares. Comment on: "Bounds on the number of functions satisfying the strict avalanche criterion" [Inform. Process. Lett. **60** (1996), no. 4, 215–219; 1 435 155] by T. W. Cusick and P. Stănică. *Information Processing Letters*, 60(5):271–275, December 8, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [Cus96, CS96c].

Yu:1992:NTD

[Yu92] Xiu Yuan Yu. A note on the trap-door knapsack public-key cryptosystem. *Gaoxiao Yingyong Shuxue Xuebao*, 7 (4):502–508, 1992. ISSN 1000-4424.

Yu:1994:KAX

[Yu94a] Tom Yu. Kerberos authentication of X connections. *The X Resource*, 9(1):237–243, January 1994. CODEN XRESEA. ISBN 1-56592-066-X. ISSN 1058-5591.

Yu:XR-9-1-237

[Yu94b] Tom Yu. Kerberos authentication of X connections. *The X Resource*, 9(1):237–243, January 1994. CODEN XRESEA. ISBN 1-56592-066-X. ISSN 1058-5591.

Yu:1999:CC

[Yu99] Maochun Yu. Chinese codebreakers, 1927–45. *Intelligence and National Security*, 14(1):201–??, 1999. ISSN 0268-4527 (print), 1743-9019 (electronic).

Yuan:1992:VLD

[Yua92] Li-Yan Yuan, editor. *Very large data bases: VLDB '92, proceedings of the 18th International Conference on Very Large Data Bases, August 23–27, 1992, Vancouver, Canada*. Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 1992. ISBN 1-55860-151-1. LCCN QA76.9.D3 I61 1992.

Yung:1985:CSP

[Yun85a] Mordechai Yung. Cryptoprotocols: Subscription to a public key, the secret blocking and the multi-player mental poker game (extended abstract). In Blakley and Chaum [BC85], pages 439–453. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=439`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Yung:1985:SUK

[Yun85b] Mordechai M. Yung. A secure and useful "keyless cryptosystem". *Information Processing Letters*, 21 (1):35–38, July 10, 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Yuval:1997:RTE

[Yuv97] Gideon Yuval. Reinventing the travois: Encryption/MAC in 30 ROM bytes. *Lecture Notes in Computer Science*, 1267: 205–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670205.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1267/12670205.pdf`.

Yang:1997:CBC

[YWC97] T'ao Yang, Chai Wah Wu, and Leon O. Chua. Cryptography based on Chua's circuits. Technical Report UCB/ERL M97/6, Electronics Research Laboratory, College of Engineering, University of California, Berkeley, Berkeley, CA, USA, January 17, 1997. 9 pp.

Yang:1999:GSP

[YWY99] Jian Zhan Yang, Yong Wang, and Xing Yi. Generating strong primes in RSA cryptosystems. *J. Wuhan Univ. Natur. Sci. Ed.*, 45 (3):303–306, 1999. CODEN WTHPDI. ISSN 0253-9888.

Yu:1989:DEB

[YY89] K. W. Yu and T. L. Yu. Data encryption based upon time reversal transformations. *The Computer Journal*, 32(3):241–245, June 1989. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Yu:1991:SED

[YY91] K. W. Yu and Tong Lai Yu. Superimposing encrypted data. *Communications of the Association for Computing Machinery*, 34(2): 48–54, February 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/102800.html`. See [BY92].

Young:1996:DSB

[YY96] A. Young and M. Yung. The dark side of black-box cryptography, or: Should we trust Capstone? *Lecture Notes in Computer Science*, 1109:89–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Young:1997:KUC

[YY97a] Adam Young and Moti Yung. Kleptography: Using cryptography against cryptography. *Lecture Notes in Computer Science*, 1233: 62–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330062.htm; http://link.springer-ny.com/link/service/series/0558/papers/1233/12330062.pdf`.

Young:1997:PKA

[YY97b] Adam Young and Moti Yung. The prevalence of kleptographic attacks on discrete-log based cryptosystems. *Lecture Notes in Computer Science*, 1294: 264–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940264.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940264.pdf`.

Young:1997:SEC

[YY97c] Adam Young and Moti Yung. Sliding encryption:

a cryptographic tool for mobile agents. *Lecture Notes in Computer Science*, 1267:230–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670230.htm; http://link.springer-ny.com/link/service/series/0558/papers/1267/12670230.pdf.

Young:1998:FLP

[YY98a] A. Young and M. Yung. Finding length-3 positive Cunningham chains and their cryptographic significance. *Lecture Notes in Computer Science*, 1423:289–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Young:1998:MBS

[YY98b] A. Young and M. Yung. Monkey: Black-box symmetric ciphers designed for MONopolizingKEYs. *Lecture Notes in Computer Science*, 1372:122–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Young:1998:ARA

[YY98c] Adam Young and Moti Yung. Auto-recoverable auto-certifiable cryptosystems. *Lecture Notes in Computer Science*, 1403:17–31, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Young:1998:MBB

[YY98d] Adam Young and Moti Yung. Monkey: Black-box symmetric ciphers designed for MON*opolizing* KEY*s*. *Lecture Notes in Computer Science*, 1372:122–133, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720122.htm; http://link.springer-ny.com/link/service/series/0558/papers/1372/13720122.pdf.

Yeo:1999:WOV

[YY99a] Boon-Lock Yeo and Minerva M. Yeung. Watermarking 3D objects for verification. *IEEE Computer Graphics and Applications*, 19(1):36–45, January/February 1999. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic). URL http://computer.org/cga/cg1999/g1036abs.htm; http://dlib.computer.org/cg/books/cg1999/pdf/g1036.pdf.

Young:1999:ARC

[YY99b] Adam Young and Moti Yung. Auto-recoverable cryptosystems with faster initialization and the escrow hierarchy. *Lecture Notes in Computer Science*, 1560:306–314, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1560/15600306.htm; http://link.springer-ny.com/link/service/series/0558/papers/1560/15600306.pdf.

Yeung:1998:DWS

[YYH98] Minerva M. Yeung, Boon-Lock L. Yeo, and Matthew Holliman. Digital watermarks — shedding light on the invisible. *IEEE Micro*, 18(6):32–41, November/December 1998. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://dlib.computer.org/mi/books/mi1998/pdf/m6032.pdf; http://www.computer.org/micro/mi1998/m6032abs.htm.

Zafiropulo:1963:RAD

[Zaf63] Jean Zafiropulo. Le rôle de l'analogie dans le déchiffrement de l'écriture mycénienne linéaire B. (French) [The role of analogy in deciphering Mycenaean linear script B]. *Dialectica: International Review of Philosophy of Knowledge*, 17(4):307–327, December 1963. CODEN ???? ISSN 0012-2017 (print), 1746-8361 (electronic).

Zajacz:1997:SCE

[Zaj97] Rita Zajacz. State-industry confrontation in encryption policy making. Thesis (M.A.), Indiana University, Bloomington, IN, USA, 1997. vi + 167 pp.

Zang:1990:ESE

[Zan90] Xiguang Zang. Enhanced substitution-permutation encryption networks. Thesis (M.S. in Computer Science), University of Wisconsin-Milwaukee, Milwaukee, WI, USA, 1990. viii + 26 pp.

Zave:1999:SDC

[Zav99] P. Zave. Systematic design of call-coverage features. *Lecture Notes in Computer Science*, 1548:23–27, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zegwaart:1993:PEM

[Zeg93] Erik Zegwaart. Privacy Enhanced Mail in more detail. *Computer Networks and ISDN Systems*, 25(Supplement 2): S63–S71, 1993. CODEN

CNISE9. ISSN 0169-7552 (print), 1879-2324 (electronic). URL gopher://erasmus.rare.nl:70/00cnre/cnre2/S063-S071.txt; zegwaart@surfnet.nl.

Zeidler:1979:DDE

[Zei79] Howard M. Zeidler. *Digital data encryption*. SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025-3493, USA, Tel: +1 415 859 6387, FAX: +1 415 859-6028, 1979. 20 pp.

Zergo:1996:UER

[Zer96a] Zergo. The use of encryption and related services with the NHSnet: a report for the NHS Executive. Report IMG E5254., Department of Health, Wetherby, West Yorkshire, UK, April 1996. 64 pp.

Zerovnik:1996:RC

[Žer96b] Janez Žerovnik. The RSA cryptosystem in 1873. *Dru vstvo Matematikov, Fizikov in Astronomov SRS. Obzornik za Matematiko in Fiziko*, 43(4):116–118, 1996. CODEN OBMFAY. ISSN 0473-7466.

Zollner:1998:MSS

[ZFK+98] J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf. Modeling the security of steganographic systems. *Lecture Notes in Computer Science*, 1525:344–354, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1525/15250344.htm; http://link.springer-ny.com/link/service/series/0558/papers/1525/15250344.pdf.

Zoellner:1998:MSS

[ZFKP98] J. Zoellner, H. Federrath, H. Klimant, and A. Pfitzmann. Modeling the security of steganographic systems. *Lecture Notes in Computer Science*, 1525:344–354, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zuquete:1996:TAC

[ZG96] Andre Zuquete and Paulo Guedes. Transparent authentication and confidentiality for stream sockets — ensuring private network communications for Unix and Windows systems. *IEEE Micro*, 16(3):34–41, May/June 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Zeng:1990:LSM

[ZH90] Ken Cheng Zeng and

Min Qiang Huang. On the linear syndrome method in cryptanalysis. *Lecture Notes in Computer Science*, 403:469–478, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zviran:1993:CPT

[ZH93] M. Zviran and W. J. Haga. A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal*, 36 (3):227–237, June 1993. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/Volume_36/Issue_03/Vol36_03.body.html#AbstractZviran.

Zhang:1991:BNK

[Zha91] Zhao Zhi Zhang. Breaking a new knapsack public key cryptosystem. *J. Systems Sci. Math. Sci.*, 11(1): 91–97, 1991. CODEN XKSHEW. ISSN 1000-0577.

Zhao:1996:WSE

[Zha96] J. Zhao. A WWW service to embed and prove digital copyright watermarks. In Danthine [Dan96], pages 695–710. LCCN ???? URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1041.html.

Zhao:1997:LT

[Zha97] J. Zhao. Look, its not there. *BYTE Magazine*, ?? (??):401–407, January 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061171.html.

Zhang:1998:TPS

[Zha98] K. Zhang. Threshold proxy signature schemes. *Lecture Notes in Computer Science*, 1396:282–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zheng:1990:PDS

[Zhe90] Yuliang Zheng. *Principles for Designing Secure Block Ciphers and One-Way Hash Functions*. PhD thesis, Yokohama National University, Yokohama, Japan, 1990. ?? pp.

Zheng:1995:HBR

[Zhe95a] Y. Zheng. How to break and repair Leighton and Micali's key agreement protocol. *Lecture Notes in Computer Science*, 950:299–305, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zheng:1995:KAP

[Zhe95b] Yuliang Zheng. On key agreement protocols based on tamper-proof hardware. *Information Processing Letters*, 53(1):49–54, January 13, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Zheng:1997:SC

[Zhe97a] Y. Zheng. The SPEED cipher. *Lecture Notes in Computer Science*, 1318: 71–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zheng:1997:DSH

[Zhe97b] Yuliang Zheng. Digital signcryption or how to achieve cost (signature and encryption) << cost(signature) + cost(encryption). *Lecture Notes in Computer Science*, 1294:165–179, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940165.htm; http://link.springer-ny.com/link/service/series/0558/papers/1294/12940165.pdf`.

Zilouchian:1998:ANF

[ZHJ98] A. Zilouchian, D. W. Howard, and T. Jordanides. An adaptive neuro-fuzzy inference System(ANFIS) approach to control of robotic manipulators. *Lecture Notes in Computer Science*, 1416:383–392, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zhou:1994:SDS

[Zho94] Fang Zhou. A survey of digital signature variations and a study of implementations using RSA and ElGamal cryptosystems. Thesis (M.S.), Computer Science Telecommunications Program. University of Missouri — Kansas City, Kansas City, MO, USA, 1994. ix + 66 pp.

Zheng:1994:RSS

[ZHS94] Yuliang Zheng, T. Hardjono, and J. Seberry. Reusing shares in secret sharing schemes. *The Computer Journal*, 37(3):199–205, ???? 1994. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Zheng:1998:HCE

[ZI98] Yuliang Zheng and Hideki Imai. How to construct efficient signcryption schemes on elliptic curves. *Information Processing Letters*, 68 (5):227–233, December 15, 1998. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Zieschang:1997:CPB

[Zie97] Thilo Zieschang. Combinatorial properties of basic encryption operations. *Lecture Notes in Computer Science*, 1233:14–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1233/12330014.htm; http://link.springer-ny.com/link/service/series/0558/papers/1233/12330014.pdf.

Zim:1948:CSW

[Zim48] Herbert S. Zim. *Codes and secret writing*. William Morrow, New York, NY, USA, 1948. vi + 154 pp. LCCN Z104 .Z5.

Zimmermann:1995:OPU

[Zim95a] Philip R. Zimmermann. *The Official PGP User's Guide*. MIT Press, Cambridge, MA, USA, 1995. ISBN 0-262-74017-6. xviii + 127 pp. LCCN TK5102.85 .Z56 1995. US$14.95. URL http://www-mitpress.mit.edu/mitp/recent-books/comp/pgp-user.html.

Zimmermann:1995:PSC

[Zim95b] Philip R. Zimmermann. *PGP: Source Code and Internals*. MIT Press, Cambridge, MA, USA, 1995. ISBN 0-262-24039-4. xxi + 907 pp. LCCN TK5102.85 .Z58 1995. US$55.00. URL http://www-mitpress.mit.edu/mitp/recent-books/comp/pgp-source.html.

Zimmermann:1996:PGPa

[Zim96a] Philip (Philip R.) Zimmermann. *Pretty good privacy 3.0 pre-alpha source code*. Warthman Associates, Palo Alto, CA, USA, preliminary release 1. edition, 1996. ISBN 0-9649654-1-0. LCCN ????

Zimmermann:1996:PGPb

[Zim96b] Philip (Philip R.) Zimmermann. *Pretty good privacy 3.0 pre-alpha source code, preliminary release 1.1: distributed at the December 14, 1996 Public Cyberpunks Meeting*. Warthman Associates, Palo Alto, CA, USA, 1996. ISBN 0-9649654-2-9. iv + 312 pp. LCCN TK5102.85Z59 1996.

Zimmermann:1998:CI

[Zim98] Philip R. Zimmermann. Cryptography on the Internet. *Scientific American*, 279(4):110–115 (Intl. ed. 82–??), October 1998. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.sciam.com/1998/1098issue/1098currentissue.html.

Zimmermann:1999:EVI

[Zim99] Reto Zimmermann. Efficient VLSI implementation of modulo ($2^n \pm 1$) addition and multiplication. In Koren and Kornerup [KK99b], pages 158–167. ISBN 0-7803-5609-8, 0-7695-0116-8, 0-7695-0118-4. ISSN 1063-6889. LCCN QA76.6 .S887 1999. URL http://euler.ecs.umass.edu/paper/final/paper-127.pdf; http://euler.ecs.umass.edu/paper/final/paper-127.ps; http://www.acsel-lab.com/arithmetic/arith14/papers/ARITH14_Zimmermann.pdf. IEEE Computer Society Order Number PR00116. IEEE Order Plan Catalog Number 99CB36336.

Zhao:1995:ERL

[ZK95] J. Zhao and E. Koch. Embedding robust labels into images for copyright protection. In Brunnstein and Sint [BS95e], pages 242–252. ISBN 3-486-23483-8 (Oldenbourg, Munchen), 3-7029-0408-5 (Oldenbourg, Wien), 3-85403-082-7 (Osterr. Computer-Ges.), 3-85403-082-7 (Osterreichische Computer Ges.). LCCN KJ118.I5 K66 1995. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1006.html.

Zhao:1996:DWS

[ZK96] Jian Zhao and Eckhard Koch. A digital watermarking system for multimedia copyright protection. In ACM [ACM96a], pages 443–444. ISBN 0-201-92140-X (Addison Wesley) (??invalid ISBN??), 0-89791-871-1 (ACM). LCCN QA76.575.A36 1996. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061170.html.

Zhao:1998:GDW

[ZK98] Jian Zhao and Eckhard Koch. A generic digital watermarking model. *Computers and Graphics*, 22(4):397–403, July–August 1, 1998. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL http://www.elsevier.com/cas/tree/store/cag/sub/1998/22/4/563.pdf.

Zhao:1998:BTT

[ZKL98] J. Zhao, E. Koch, and C. Luo. In business today and tomorrow. *Communications of the Association for Computing Machinery*, 41(7):67–72, July 1998. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073184.html.

Zhao:1999:DWW

[ZKOY99] Jian Zhao, Eckhard Koch, Joe O'Ruanaidh, and Minerva M. Yeung. Digital watermarking: what will it do for me? And what it won't! In ACM [ACM99c], pages 153–155. ISBN 0-201-48560-5. ISSN 1069-529X. LCCN T385 .S54 1999. URL http://www.acm.org/pubs/citations/proceedings/graph/311625/p153-zhao/. ACM order number 428990.

Zeng:1997:RRO

[ZL97] Wenjun Zeng and Bede Liu. On resolving rightful ownerships of digital images by invisible watermarks. In IEEE [IEE97h], pages 552–555. ISBN 0-8186-8183-7, 0-8186-8184-5 (case). LCCN TK8315 .I16 1997. Three volumes. IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144.

Zhou:1999:SPP

[ZL99] J. Zhou and K.-Y. Lam. A secure pay-per-view scheme for Web-based video service. *Lecture Notes in Computer Science*, 1560: 315–326, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

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:1990:CBC

[ZMI90] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses (extended abstract). *Lecture Notes in Computer Science*, 435:461–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350461.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350461.pdf.

Zheng:1991:DBT

[ZMI91] Y. Zheng, T. Matsumoto, and H. Imai. Duality between two cryptographic primitives. *Lecture Notes in Computer Science*, 508: 379–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zolman:1993:BSJ

[Zol93] Leor Zolman. Building a secure journal/logging utility with encryption. *Sys Admin: The Journal for UNIX Systems Administrators*, 2(6):75–??, November/December 1993. CODEN SYADE7. ISSN 1061-2688.

Zorpette:1987:BEC

[Zor87] Glenn Zorpette. Breaking the enemy's code: British intelligence deciphered Germany's top-secret military communications with Colossus, an early vacuum-tube computer. *IEEE Spectrum*, 24 (9):47–51, September 1987. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Zheng:1993:HOH

[ZPS93] Y. Zheng, J. Pieprzyk, and J. Seberry. HAVAL — a one-way hashing algorithm with variable length and output. In Seberry and Zheng [SZ93], pages 83–104. CODEN LNCSD9. ISBN 0-387-57220-1 (New York), 3-540-57220-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 A87 1992.

Zhu:1996:PKC

[ZPY96] Yuefei Zhu, Dingyi Pei, and Dingfeng Ye. Public key cryptosystems based on imaginary quadratic algebraic function fields. *Progr. Natur. Sci. (English Ed.)*, 6(2):217–226, 1996. ISSN 1002-0071.

Zheng:1993:PAA

[ZS93] Y. Zheng and J. Seberry. Practical approaches to attaining security against adaptively chosen ciphertext attacks. *Lecture Notes in Computer Science*, 740: 292–304, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zwiggelaar:1999:DCM

[ZTR99] R. Zwiggelaar, C. J. Taylor, and C. M. E. Rubin. Detection of the central mass of spiculated lesions — signature normalisation and model data aspects. *Lecture Notes in Computer Science*, 1613:406–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zukowski:1998:JTUb

[Zuk98a] John Zukowski. Java tip 46: Use Java 1.2's Authenticator class. *JavaWorld: IDG's magazine for the Java community*, 3(2): ??, February 1998. CODEN ???? ISSN 1091-8906. URL `http://www.javaworld.com/javaworld/javatips/jw-javatip46.htm`.

Zukowski:1998:JTUa

[Zuk98b] John Zukowski. Java tip 47: URL authentication revisited. *JavaWorld: IDG's* *magazine for the Java community*, 3(2):??, February 1998. CODEN ???? ISSN 1091-8906. URL http://www.javaworld.com/javaworld/javatips/jw-javatip47.htm.

Zunic:1998:MCI

[Zun98] Nevenko Zunic. The MARS cipher — IBM submission to AES. In National Institute of Standards and Technology [Nat98], page ?? ISBN ???? LCCN ???? URL http://www.research.ibm.com/security/mars.html. No slides for the conference talk are available.

Zachariasen:1999:OAE

[ZW99] M. Zachariasen and P. Winter. Obstacle-avoiding Euclidean Steiner trees in the plane: An exact algorithm. *Lecture Notes in Computer Science*, 1619:282–295, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zwiers:1998:CTD

[Zwi98] J. Zwiers. Compositional transformational design for concurrent programs. *Lecture Notes in Computer Science*, 1536:609–631, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zeng:1990:LCT

[ZYR90] Ken Cheng Zeng, C. H. Yang, and T. R. N. Rao. On the linear consistency test (LCT) in cryptanalysis with applications. *Lecture Notes in Computer Science*, 435:164–174, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zeng:1991:ILS

[ZYR91] K. Zeng, C. H. Yang, and T. R. N. Rao. An improved linear syndrome algorithm in cryptanalysis with applications. *Lecture Notes in Computer Science*, 537:34–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zeng:1991:PBG

[ZYWR91] Kencheng Zeng, Chung-Huang Yang, Dah-Yea Wei, and T. R. N. Rao. Pseudorandom bit generators in stream-cipher cryptography. *Computer*, 24(2):8–17, February 1991. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Zhang:1995:GCG

[ZZ95] Xian-Mo Zhang and Yuliang Zheng. GAC — the criterion for global avalanche characteristics of cryptographic functions.

J.UCS: Journal of Universal Computer Science, 1(5):320–337, May 28, 1995. ISSN 0948-6968. URL http://www.iicm.edu/gac_the_criterion_for_global_avalanche_characteristics_of_cryptographic_functions.

Zhang:1996:DCC

[ZZ96] Xian-Mo Zhang and Yuliang Zheng. On the difficulty of constructing cryptographically strong substitution boxes. *J.UCS: Journal of Universal Computer Science*, 2(3):147–162, March 28, 1996. ISSN 0948-6968. URL http://www.iicm.edu/jucs_2_3/on_the_difficulty_of.

Zhang:1997:DBF

[ZZI97] X.-M. Zhang, Y. Zheng, and H. Imai. Duality of Boolean functions and its cryptographic significance. *Lecture Notes in Computer Science*, 1334:159–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).