A Bibliography of Papers in *Lecture Notes in Computer Science* (1990)

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, beebe@ieee.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/

29 July 2017
Version 1.10

Title word cross-reference

References

Diffie:1990:APK

[1] 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`.

Galil:1990:SPK

[2] 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`.

Brassard:1990:HIS

[3] Gilles Brassard. How to improve signature schemes. *Lecture Notes in Computer Science*, 434:16–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340016.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340016.pdf`.

Jaburek:1990:GGP

[4] 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.

Gunther:1990:IBK

[5] Christoph G. Günther. An identity-based key-exchange protocol. *Lecture Notes in Computer Science*, 434:29–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340029.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340029.pdf.

Bauspiess:1990:HKA

[6] 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.

Isselhorst:1990:UFP

[7] 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.

Frankel:1990:PPL

[8] Yair Frankel. A practical protocol for large group oriented networks. *Lecture Notes in Computer Science*, 434:56–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340056.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340056.pdf.

Lloyd:1990:CFS

[9] Sheelagh Lloyd. Counting functions satisfying a higher order strict avalanche criterion. *Lecture Notes in Computer Science*, 434:63–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340063.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340063.pdf.

Davida:1990:KDS

[10] 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.

Pieprzyk:1990:NLE

[11] Józef P. Pieprzyk. Non-linearity of exponent permutations. *Lecture Notes in Computer Science*, 434:80–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340080.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340080.pdf.

Sgarro:1990:IDB

[12] 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.

Quisquater:1990:BHF

[13] Jean-Jacques Quisquater and Marc Girault. $2n$-bit hash-functions using n-bit symmetric block cipher algorithms. *Lecture Notes in Computer Science*, 434:102–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). 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.

Mjolsnes:1990:STD

[14] Stig F. Mjølsnes. A simple technique for diffusing cryptoperiods. *Lecture Notes in Computer Science*, 434:110–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340110.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340110.pdf.

Burmester:1990:GZK

[15] Mike V. D. Burmester, Yvo Desmedt, Fred Piper, and Michael Walker. A general zero-knowledge scheme. *Lecture Notes in Computer Science*, 434:122–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340122.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340122.pdf.

Okamoto:1990:DZKa

[16] Tatsuaki Okamoto and Kazuo Ohta. Divertible zero knowledge interactive proofs and commutative random self-reducibility. *Lecture Notes in Computer Science*, 434:134–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340134.htm; http://

link.springer-ny.com/link/service/series/0558/papers/0434/04340134.pdf.

Crepeau:1990:VDS

[17] 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.

Boyar:1990:PZK

[18] Joan Boyar, Katalin Friedl, and Carsten Lund. Practical zero-knowledge proofs: Giving hints and using deficiencies. *Lecture Notes in Computer Science*, 434:155–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340155.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340155.pdf.

Stern:1990:AFS

[19] Jacques Stern. An alternative to the Fiat–Shamir protocol. *Lecture Notes in Computer Science*, 434:173–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340173.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340173.pdf.

Brassard:1990:SZK

[20] Gilles Brassard and Claude Crépeau. Sorting out zero-knowledge. *Lecture Notes in Computer Science*, 434:181–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340181.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340181.pdf.

Brassard:1990:ENC

[21] Gilles Brassard, Claude Crépeau, and Moti Yung. Everything in NP can be argued in *Perfect* zero-knowledge in a *Bounded* number of rounds (extended abstract). *Lecture Notes in Computer Science*, 434:192–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340192.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340192.pdf.

Yung:1990:ZKP

[22] Moti Yung. Zero-knowledge proofs of computational power (extended summary). *Lecture Notes in Computer Science*, 434:196–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340196.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340196.pdf.

denBoer:1990:MEM

[23] Bert den Boer. More efficient match-making and satisfiability: *The Five Card Trick*. *Lecture Notes in Computer Science*, 434:208–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340208.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340208.pdf.

Vandemeulebroecke:1990:SCB

[24] 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.

Cnudde:1990:CPP

[25] Hedwig Cnudde. Cryptel — the practical protection of an existing electronic mail system. *Lecture Notes in Computer Science*, 434:237–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340237.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340237.pdf.

VanAuseloos:1990:TSS

[26] Jan Van Auseloos. Technical security: The starting point. *Lecture Notes in Computer Science*, 434:243–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340243.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340243.pdf.

Siuda:1990:SOD

[27] Charles Siuda. Security in open distributed processing. *Lecture Notes in Computer Science*, 434:249–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340249.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340249.pdf.

Vandewalle:1990:ECC

[28] 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.

Antoine:1990:LRF

[29] Mireille Antoine, Jean-François Brakeland, Marc Eloy, and Yves Poullet. Legal requirements facing new signature technology (invited). *Lecture Notes in Computer Science*, 434:273–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340273.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340273.pdf.

Chaum:1990:OCC

[30] David Chaum. Online cash checks. *Lecture Notes in Computer Science*, 434:288–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340288.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340288.pdf.

Chaum:1990:EOE

[31] David Chaum, Bert den Boer, Eugène van Heyst, Stig F. Mjølsnes, and Adri Steenbeek. Efficient offline electronic checks (extended abstract). *Lecture Notes in Computer Science*, 434:294–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340294.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340294.pdf.

Waidner:1990:USR

[32] Michael Waidner. Unconditional sender and recipient untraceability in spite of active attacks. *Lecture Notes in Computer Science*, 434:302–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340302.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340302.pdf.

Bos:1990:DDD

[33] Jurjen N. E. Bos and Bert den Boer. Detection of disrupters in the DC protocol. *Lecture Notes in Computer Science*, 434:320–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340320.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340320.pdf.

Flajolet:1990:RMS

[34] Philippe Flajolet and Andrew M. Odlyzko. Random mapping statistics (invited). *Lecture Notes in Computer Science*, 434:329–354, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340329.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340329.pdf; 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.

Lenstra:1990:FEM

[35] Arjen K. Lenstra and Mark S. Manasse. Factoring by electronic mail. *Lecture Notes in Computer Science*, 434:355–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340355.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340355.pdf.

Wiener:1990:CSR

[36] 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.

Pfitzmann:1990:HBD

[37] Birgit Pfitzmann and Andreas Pfitzmann. How to break the direct RSA-implementation of MIXes. *Lecture Notes in Computer Science*, 434:373–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). 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.

Jendal:1990:ITT

[38] Hakon N. Jendal, Yves J. B. Kuhn, and James L. Massey. An information-theoretic treatment of homophonic substitution. *Lecture Notes in Computer Science*, 434:382–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340382.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340382.pdf.

Wichmann:1990:CMR

[39] 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.

Bertilsson:1990:CVE

[40] Michael Bertilsson, Ernest F. Brickell, and Ingemar Ingemarsson. Cryptanalysis of video encryption based on space-filling curves. *Lecture Notes in Computer Science*, 434:403–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). 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.

Zheng:1990:IOR

[41] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. Impossibility and optimally results on constructing pseudorandom permutations (extended abstract). *Lecture Notes in Computer Science*, 434:412–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340412.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340412.pdf.

Rueppel:1990:SSP

[42] Rainer A. Rueppel. On the security of Schnorr's pseudo random generator. *Lecture Notes in Computer Science*, 434:423–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340423.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340423.pdf.

Quisquater:1990:HECa

[43] Jean-Jacques Quisquater and Jean-Paul Delescaille. How easy is collision search? application to DES (extended summary). *Lecture Notes in Computer Science*, 434:429–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340429.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340429.pdf.

Simmons:1990:PSS

[44] 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.

Brickell:1990:SIS

[45] 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.

DeSoete:1990:CAS

[46] 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.

Beutelspacher:1990:HSN

[47] Albrecht Beutelspacher. How to say “no”. *Lecture Notes in Computer Science*, 434:491–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340491.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340491.pdf.

Godlewski:1990:KMA

[48] 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.

Gunther:1990:PGR

[49] Christoph G. Günther. Parallel generation of recurring sequences. *Lecture Notes in Computer Science*, 434:503–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340503.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340503.pdf.

Niederreiter:1990:KSG

[50] Harald Niederreiter. Keystream sequences with a good linear complexity profile for every starting point. *Lecture Notes in Computer Science*, 434:523–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340523.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340523.pdf.

Beth:1990:CPR

[51] Thomas Beth and Zong-Duo Dai. On the complexity of pseudo-random sequences — or: If you can describe a sequence it can’t be random. *Lecture Notes in Computer Science*, 434:533–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340533.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340533.pdf.

Dai:1990:FFD

[52] Zong-Duo Dai and Kencheng Zeng. Feedforward functions defined by de brujin sequences. *Lecture Notes in Computer Science*, 434:544–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340544.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340544.pdf.

Meier:1990:NCC

[53] 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.

Chan:1990:LCF

[54] Agnes Hui Chan, Mark Goresky, and Andrew Klapper. On the linear complexity of feedback registers (extended abstract). *Lecture Notes in Computer Science*, 434:563–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340563.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340563.pdf.

Wang:1990:LCP

[55] Muzhong Wang. Linear complexity profiles and continued fractions. *Lecture Notes in Computer Science*, 434:571–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340571.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340571.pdf.

Forre:1990:FCA

[56] Réjane Forré. A fast correlation attack on nonlinearly feed-forward filtered shift-register sequences. *Lecture Notes in Computer Science*, 434:586–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340586.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340586.pdf.

Buchmann:1990:CEN

[57] Johannes A. Buchmann, Stephen Düllmann, and Hugh C. Williams. On the complexity and efficiency of a new key exchange system. *Lecture Notes in Computer Science*, 434:597–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340597.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340597.pdf.

Boyd:1990:NMK

[58] 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.

Morain:1990:ATN

[59] François Morain. Atkin's test: News from the front. *Lecture Notes in Computer Science*, 434:626–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-

tronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340626.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340626.pdf.

Maurer:1990:FGS

[60] 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.

Duhoux:1990:DBA

[61] 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.

Bosma:1990:FPT

[62] Wieb Bosma and Marc Paul van der Hulst. Faster primality testing (extended abstract). *Lecture Notes in Computer Science*, 434:652–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340652.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340652.pdf.

Hwang:1990:PKA

[63] 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.

Quisquater:1990:ZKP

[64] Jean-Jacques Quisquater and André Bouckaert. Zero-knowledge procedures for confidential access to medical records (extended summary). *Lecture Notes in Computer Science*, 434:662–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340662.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340662.pdf.

DomingoiFerrer:1990:FSK

[65] 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 (elec-

tronic). 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.

Roggeman:1990:VFS

[66] Yves Roggeman. Varying feedback shift registers. *Lecture Notes in Computer Science*, 434:670–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340670.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340670.pdf.

Gollmann:1990:CC

[67] 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.

Schnorr:1990:EISa

[68] 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.

Waidner:1990:DCD

[69] 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.

Carter:1990:SCL

[70] Glyn Carter. Some conditions on the linear complexity profiles of certain binary sequences. *Lecture Notes in Computer Science*, 434:691–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340691.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340691.pdf.

Brown:1990:DPT

[71] 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.

Agnew:1990:FEC

[72] 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.

Anonymous:1990:AIa

[73] Anonymous. Author index. *Lecture Notes in Computer Science*, 434:709–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/papers/0434/0434ind.pdf.

Kahn:1990:KGN

[74] David Kahn. Keying the German Navy's Enigma (invited). *Lecture Notes in Computer Science*, 435:2–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350002.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350002.pdf.

Desmedt:1990:MCS

[75] Yvo Desmedt. Making conditionally secure cryptosystems unconditionally abuse-free in a general context (extended abstract). *Lecture Notes in Computer Science*, 435:6–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350006.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350006.pdf.

Damgaard:1990:EBC

[76] Ivan Bjerre Damgård. On the existence of bit commitment schemes and zero-knowledge proofs. *Lecture Notes in Computer Science*, 435:17–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350017.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350017.pdf.

Brand:1990:PNU

[77] 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.

Kohl:1990:UEK

[78] 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.

Feldmeier:1990:UPS

[79] David C. Feldmeier and Philip R. Karn. UNIX password security — ten years later (invited). *Lecture Notes in Computer Science*, 435:44–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350044.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350044.pdf.

Smith:1990:PPC

[80] 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.

Barrett:1990:SDU

[81] 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.

Chan:1990:QSP

[82] Agnes Hui Chan and Richard A. Games. On the quadratic spans of periodic sequences. *Lecture Notes in Computer Science*, 435:82–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350082.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350082.pdf.

Jansen:1990:SFS

[83] Cees J. A. Jansen and Dick E. Boekee. The shortest feedback shift register that can generate a given sequence. *Lecture Notes in Computer Science*, 435:90–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350090.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350090.pdf.

Maurer:1990:PLR

[84] Ueli M. Maurer and James L. Massey. Perfect local randomness in pseudo-random sequences. *Lecture Notes in Computer Science*, 435:100–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350100.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350100.pdf.

Goldreich:1990:SPD

[85] Oded Goldreich and Hugo Krawczyk. Sparse pseudorandom distributions (extended abstract). *Lecture Notes in Computer Science*, 435:113–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350113.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350113.pdf.

Naor:1990:BCU

[86] Moni Naor. Bit commitment using pseudo-randomness (extended abstract). *Lecture Notes in Computer Science*, 435:128–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350128.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350128.pdf.

Krawczyk:1990:HPC

[87] 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.

Preneel:1990:CTA

[88] 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.

Zeng:1990:LCT

[89] Kencheng 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–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350164.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350164.pdf.

Fiat:1990:BR

[90] 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.

Bender:1990:IEC

[91] Andreas Bender and Guy Castagnoli. On the implementation of elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 435:186–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350186.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350186.pdf.

Bellare:1990:NPD

[92] 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–??, 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.

Chaum:1990:US

[93] David Chaum and Hans van Antwerpen. Undeniable signatures. *Lecture Notes in Computer Science*, 435:212–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350212.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350212.pdf.

Merkle:1990:CDS

[94] Ralph C. Merkle. A certified digital signature (subtitle: That antique paper from 1979). *Lecture Notes in Computer Science*, 435:218–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). 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.

Schnorr:1990:EISb

[95] Claus P. Schnorr. Efficient identification and signatures for smart cards. *Lecture Notes in Computer Science*, 435:239–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350239.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350239.pdf.

Soete:1990:SSV

[96] Marijke De Soete, Jean-Jacques Quisquater, and Klaus Vedder. A signature with

shared verification scheme. *Lecture Notes in Computer Science*, 435:253–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350253.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350253.pdf.

Even:1990:LLD

[97] 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.

Brickell:1990:CIS

[98] 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.

Laih:1990:DTS

[99] Chi-Sung Laih, Lein Harn, Jau-Yien Lee, and Tzonelih Hwang. Dynamic threshold scheme based on the definition of cross-product in an N-dimensional linear space. *Lecture Notes in Computer Science*, 435:286–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350286.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350286.pdf.

Chor:1990:SSI

[100] 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.

Desmedt:1990:TC

[101] Yvo Desmedt and Yair Frankel. Threshold cryptosystems. *Lecture Notes in Computer Science*, 435:307–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350307.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350307.pdf.

Chick:1990:FAC

[102] Gerald C. Chick and Stafford E. Tavares. Flexible access control with master keys. *Lecture Notes in Computer Science*, 435:316–??, 1990. CODEN LNCSD9.

ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350316.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350316.pdf.

Tatebayashi:1990:KDP

[103] Makoto Tatebayashi, Natsume Matsuzaki, and David B. Newman, Jr. Key distribution protocol for digital mobile communication systems. *Lecture Notes in Computer Science*, 435:324–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350324.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350324.pdf.

Buchmann:1990:KES

[104] Johannes A. Buchmann and Hugh C. Williams. A key exchange system based on real quadratic fields (extended abstract). *Lecture Notes in Computer Science*, 435:335–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350335.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350335.pdf.

Yacobi:1990:KDS

[105] Yacov Yacobi and Zahava Shmuely. On key distribution systems. *Lecture Notes in Computer Science*, 435:344–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350344.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350344.pdf.

Nelson:1990:SAE

[106] 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.

Brickell:1990:SHI

[107] 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.

Findlay:1990:MEU

[108] Paul A. Findlay and Brian A. Johnson. Modular exponentiation using recursive sums of residues. *Lecture Notes in Computer Science*, 435:371–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-

ny.com/link/service/series/0558/bibs/0435/04350371.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350371.pdf.

Morita:1990:FMM

[109] Hikaru Morita. A fast modular-multiplication algorithm based on a higher radix. *Lecture Notes in Computer Science*, 435:387–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350387.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350387.pdf.

Bos:1990:ACH

[110] Jurjen N. E. Bos and Matthijs J. Coster. Addition chain heuristics. *Lecture Notes in Computer Science*, 435:400–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350400.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350400.pdf.

Quisquater:1990:HECb

[111] Jean-Jacques Quisquater and Jean-Paul Delescaille. How easy is collision search. new results and applications to DES (abstract and results). *Lecture Notes in Computer Science*, 435:408–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350408.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350408.pdf.

Damgaard:1990:DPH

[112] Ivan Bjerre Damgård. A design principle for hash functions. *Lecture Notes in Computer Science*, 435:416–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350416.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350416.pdf.

Merkle:1990:OWH

[113] Ralph C. Merkle. One way hash functions and DES. *Lecture Notes in Computer Science*, 435:428–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350428.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350428.pdf.

Magliveras:1990:PCP

[114] Spyros S. Magliveras and Nasir D. Memon. Properties of cryptosystem PGM. *Lecture Notes in Computer Science*, 435:447–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350447.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350447.pdf.

Zheng:1990:CBC

[115] 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.

Okamoto:1990:DZKb

[116] 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.

Ben-Or:1990:EIS

[117] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Efficient identification schemes using two prover interactive proofs. *Lecture Notes in Computer Science*, 435:498–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350498.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350498.pdf.

Boyar:1990:CCZ

[118] Joan Boyar and René Peralta. On the concrete complexity of zero-knowledge proofs. *Lecture Notes in Computer Science*, 435:507–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350507.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350507.pdf.

Feige:1990:ZKP

[119] Uriel Feige and Adi Shamir. Zero knowledge proofs of knowledge in two rounds. *Lecture Notes in Computer Science*, 435:526–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350526.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350526.pdf.

Kilian:1990:MRZ

[120] Joe Kilian, Silvio Micali, and Rafail Ostrovsky. Minimum resource zero-knowledge proofs (extended abstract). *Lecture Notes in Computer Science*, 435:545–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350545.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350545.pdf.

Bellare:1990:NIO

[121] Mihir Bellare and Silvio Micali. Non-interactive oblivious transfer and applications. *Lecture Notes in Computer Science*, 435:547–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350547.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350547.pdf.

Beaver:1990:MPT

[122] Donald Beaver. Multiparty protocols tolerating half faulty processors. *Lecture Notes in Computer Science*, 435:560–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350560.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350560.pdf.

Cleve:1990:CGD

[123] Richard Cleve. Controlled gradual disclosure schemes for random bits and their applications. *Lecture Notes in Computer Science*, 435:573–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350573.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350573.pdf.

Beaver:1990:MCF

[124] Donald Beaver and Shafi Goldwasser. Multiparty computation with faulty majority. *Lecture Notes in Computer Science*, 435:589–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350589.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350589.pdf.

Chaum:1990:SDA

[125] David Chaum. The spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities. *Lecture 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.

Bellare:1990:SSK

[126] 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.

Shamir:1990:EIS

[127] Adi Shamir. An efficient identifica-

tion scheme based on permuted kernels (extended abstract). *Lecture Notes in Computer Science*, 435:606–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350606.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350606.pdf`.

Ostrovsky:1990:ESP

[128] Rafail Ostrovsky. An efficient software protection scheme (abstract). *Lecture Notes in Computer Science*, 435:610–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350610.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350610.pdf`.

Adams:1990:GBE

[129] Carlisle M. Adams and Stafford E. Tavares. Good S-boxes are easy to find. *Lecture Notes in Computer Science*, 435:612–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350612.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350612.pdf`.

White:1990:CDP

[130] Steve R. White. Convert distributed processing with computer viruses. *Lecture Notes in Computer Science*, 435:616–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350616.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350616.pdf`.

Price:1990:PDS

[131] Wyn L. Price. Progress in data security standardisation. *Lecture Notes in Computer Science*, 435:620–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350620.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350620.pdf`.

Miyaguchi:1990:FCC

[132] Shoji Miyaguchi. The FEAL- 8 cryptosystem and a call for attack. *Lecture Notes in Computer Science*, 435:624–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350624.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350624.pdf`.

Quisquater:1990:HEZ

[133] Jean-Jacques Quisquater, Louis C. Guillou, and Thomas A. Berson. How to explain zero-knowledge protocols to your children. *Lecture Notes in Computer Science*, 435:628–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-`

ny.com/link/service/series/0558/
bibs/0435/04350628.htm; http://
link.springer-ny.com/link/service/
series/0558/papers/0435/04350628.
pdf.

Anonymous:1990:AIb

[134] Anonymous. Author index. *Lecture Notes in Computer Science*, 435:633–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/papers/0435/0435ind.pdf.