Bibliography of Papers from Selected 663

A.1 Asiacrypt/Auscrypt Proceedings 663

AUSCRYPT ’92. 665

ASIACRYPT 91. 664

A.2 Crypto Proceedings 667

A.3 Eurocrypt Proceedings 684

Advances in Cryptology - Proceedings of 684

Advances in Cryptology - EUROCRYPT 87, ... 687

EUROCRYPT 86, Linkijping, Sweden. 686

Advances in Cryptology-EUROCRYPT 89, ... 689

Advances in Cryptology-EUROCRYPT 88, ... 688

Advances in Cryptology - EUROCRYPT 90, ... 690

Advances in Cryptology - EUROCRYPT 92, ... 693

Advances in Cryptology - EUROCRYPT 91, ... 692

Advances in Cryptology - EUROCRYPT 94, ... 695

Advances in Cryptology - EUROCRYPT 93, ... 694

Advances in Cryptology - EUROCRYPT 96, ... 697

Advances in Cryptology-EUROCRYPT 95, ... 696

Fast Software Encryption: Second Internatio 699

Fast Software Encryption: Third International 699

ADVANCES IN CRYPTOGRAPHY-A Report on . 667

Advances in Cryptology - ASIACRYPT 94. 666

Advances in Cryptology - Proceedings of 669

Advances in Cryptology - Proceedings of 668

Advances in Cryptology - CRYPTO 85. 671

Advances in Cryptology - Proceedings of 670

Advances in Cryptology - CRYPTO 87. 673

Advances in Cryptology - CRYPTO 86. 672

Advances in Cryptology - CRYPTO 89. 675

Advances in Cryptology - CRYPTO 88. 674

Advances in Cryptology - CRYPTO 91. 677

Advances in Cryptology - CRYPTO 90. 676

Advances in Cryptology - CRYPTO 92. 678

Advances in Cryptology - CRYPTO 94. 681

Advances in Cryptology - CRYPTO 93. 680

Advances in Cryptology - CRYPTO 96. 683

Advances in Cryptology - CRYPTO 95. 682

Advances in Cryptology - EUROCRYPT 85, ... 685

A.4 Fast Software Encryption Proceedings ... 698

Fast Software Encryption: Cambridge 698

A.5 Journal of Cryptology papers.................... 700
Journal of Cryptology 700

References... 703

Index.. 62

Appendix A

Bibliography of Papers from Selected Cryptographic Forums

Contents in Brief

A.1 Asiacrypt/Auscrypt Proceedings 663
A.2 Crypto Proceedings 667
A.3 Eurocrypt Proceedings 684
A.4 Fast Software Encryption Proceedings 698
A.5 Journal of Cryptology papers 700

A.1 Asiacrypt/Auscrypt Proceedings

Advances in Cryptology – **AUSCRYPT '90.** Springer-Verlag LNCS 453 (1990).
Editors: J. Seberry and J. Pieprzyk.

V.S. Alagar, Range equations and range matrices: A study in statistical database security, 360–385.
M. Ames, Secure cryptographic initialization, 451462.
M.H.G. Anthony, K.M. Martin, J. Seberry, P. Wild, Some remarks on authentication systems, 122-139.
L. Brown, J. Pieprzyk, J. Seberry, LOKZ – a cryptographic primitive for authentication and secrecy applications, 229-236.
L. Brown, J. Seberry, Key scheduling in DES type cryptosystems, 221-228.
J.M. Carroll, The three faces of information security, 433-450.
D. Chaum, Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms, 246-264.
R.H. Cooper, W. Patterson, RSA as a benchmark for multiprocessor machines, 356-359.
Z.-D. Dai, K. Zeng, Continued fractions and Berlekamp-Massey algorithm, 24-31.
E. Dawson, B. Goldburg, Universal logic sequences, 426432.
C. Ding, Lower bounds on the weight complexities of cascaded binary sequences, 3943.
R. Ferreira, The practical application of state of the art security in real environments, 334-355.
K. Gaarder, E. Sneklcenes, On the formal analysis of PKCS authentication protocols, 106-121.
W. Geiselmann, D. Gollmann, *VLSI design* for exponentiation in $GF(2^n)$, 398-405.
M. Girault, A (non-practical) three-pass identification protocol using coding theory, 265-272.
G. Guang, Nonlinear generators of binary sequences with controllable complexity and double key, 32-36.
H. Gustafson, E. Dawson, B. Caelli, Comparison of block ciphers, 208-220.
T. Hardjono, Record encryption in distributed databases, 386-395.
B. Hayes, Anonymous one-time signatures and Aexible untraceable electronic cash, 294-305.

M. Kwan, J. Pieprzyk, A general purpose technique for locating key scheduling weaknesses in DES-like cryptosystems, 237-246.

C.-S. Laih, L. Ham, Generalized threshold cryptosystems, 159-166.

C.-S. Laih, S.-M. Yen, L. Ham, Two efficient server-aided secret computation protocols based on the addition sequence, 450-459.

H.-Y. Lin, L. Ham, A generalized secret sharing scheme with cheater detection, 149-158.

J. Meijers, J. van Tilburg, Extended majority voting and private-key algebraic-code encryptions, 288-298.

A. Miyaji, On ordinary elliptic curve cryptosystems, 460–469.

H. Miyano, A method to estimate the number of ciphertext pairs for differential cryptanalysis, 5 l-58.

J.-I. Mizusawa, ZC-cards and telecommunication services, 253-264.

S. Mjølsnes, Privacy, cryptographic pseudonyms, and the state of health, 493-494.

H. Morita, K. Ohta, S. Miyaguchi, Results of switching-closure-test on FEAL, 247-252.

W. Ogata, K. Kurosawa, On claw free families, 111-123.

K. Ohta, T. Okamoto, A digital multisignature scheme based on the Fiat-Shamir scheme, 139-148.

T. Okamoto, An extension of zero-knowledge proofs and its applications, 368-38 1.

J. Pieprzyk, B. Sadeghiyan, Optimal perfect randomizers, 225-236.

M.Y. Rhee, Research activities on cryptology in Korea, 179-193.

R.L. Rivest, Cryptography and machine learning, 427439.

R.L. Rivest, On *NIST's* proposed digital signature standard, 481-484.

B. Sadeghiyan, J. Pieprzyk, On necessary and sufficient conditions for the construction of super *pseudo*random permutations, 194-209.

B. Sadeghiyan, Y. Zheng, J. Pieprzyk, How to construct a family of strong one-way permutations, 97-110.

R. Safavi-Naini, Feistel type authentication codes, 167-178.

T. Saito, K. Kurosawa, K. Sakurai, 4 move perfect ZKZP of knowledge with no assumption, 321-330.

A. Shimbo, S.-I. Kawamura, Cryptanalysis of several conference key distribution schemes, 265-276.

C. Shu, T. Matsumoto, H. Imai, A multi-purpose proof system -for identity and membership proofs, 397–411

M.-J. Toussaint, Formal verification of probabilistic properties in cryptographic protocols, 412-426.

J.-H. Yang, Z.-D. Dai, K.-C. Zeng, The data base of selected permutations, 73-81.

Y. Zheng, T. Hardjono, J. Pieprzyk, Sibling intractable function families and their applications, 124-138.

Advances in Cryptology – **AUSCRYPT '92.** Springer-Verlag LNCS 718 (1993).
Editors: J. Seberry and Y. Zheng.

M. Bertilsson, I. Ingemarsson, A construction ofpractical secret sharing schemes using linear block codes, 67-79.

M. Cerecedo, T. Matsumoto, H. Imai, Non-interactive generation of shared pseudorandom sequences, 385-396.

C.-C. Chang, T.-C. Wu, C.-P. Chen, The design of a conference key distribution system, 459–466.

C. Charnes, J. Pieprzyk, Linear nonequivalence versus nonlinearity, 156-164.

L. Condie, Prime generation with the Demytko-Miller-Trbovich algorithm, 413–421.

E. Dawson, Cryptanalysis of summation generator, 209-215.

Y. Desmedt, Threshold cryptosystems, 3-14.

Y. Desmedt, J. Seberry, Practical proven secure authentication with arbitration, 27-32.

J. Detombe, S.E. Tavares, Constructing large cryptographically strong S-boxes, 165-l 8 1.

A. Fujioka, T. Okamoto, K. Ohta, A practical secret voting scheme for large scale elections, 244-25 1.

T. Hardjono, Y. Zheng, A practical digital multisignature scheme based on discrete logarithms, 122-132.

L. Ham, S. Yang, Group-oriented undeniable signature schemes without the assistance of a mutually trusted party, 133-142.

L. Ham, S. Yang, Public-key cryptosystem based on the discrete logarithm problem, 469476.

A.P.L. Hiltgen, Construction of feebly-one-way families of permutations, 422-434.

W.-A. Jackson, K.M. Martin, Cumulative arrays and geometric secret sharing schemes, 48-55.

A. Klapper, The vulnerability of geometric sequences based on fields of odd characteristic, 327-338.

L.R. Knudsen, Cryptanalysis of *LOKI91*, 196-208.

C.J.A. Jansen, D.E. Boekee, A binary sequence generator based on Ziv-Lempel source coding, 156-164.

C.J.A. Jansen, D.E. Boekee, On the significance of the directed acyclic word graph in cryptology, 318–326.

S.J. Knapskog, Formal specification and verification of secure communication protocols, 58-73.

K. Koyama, Direct demonstration of the power to break public-key cryptosystems, 14–21.

P.J. Lee, Secure user access control for public networks, 46-57.

R. Lidl, W.B. Miiller, A note on strong Fibonacci pseudoprimes, 3 1 l-3 17.

A. Menezes, S. Vanstone, The implementation of elliptic curve cryptosystems, 2-13.

M.J. Mihaljević, J.D. Golić, A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence, 165-175.

H. Morita, A fast modular-mulitplication module for smart cards, 406–409.

M. Newberry, *Minòs:* Extended user authentication, 410-423.

K. Ohta, K. Koyama, Meet-in-the-middle attack on digital signature schemes, 140–154.

J. Pieprzyk, X.-M. Zhang, Permutation generators of alternating groups, 237-244.

R. Safavi-Naini, Parallel generation ofpseudo-random sequences, 176-193.

H. Shizuya, K. Koyama, T. Itoh, Demonstrating possession without revealing factors and its application, 273-293.

J.C.A. van der Lubbe, D.E. Boekee, KEYMEX: An expert system for the design of key management schemes, 96-103.

V. Varadharajan, Network security policy models, 74-95.

Y.Y. Xian, Dyadic matrices and their potential significance in cryptography, 308-310.

Y.Y. Xian, K-M sequence is forwardly predictable, 37-38.

K. Zeng, M. Huang, Solving equations in sequences, 327-332.

K. Zeng, C.H. Yang, T.R.N. Rao, Large primes in stream cipher cryptography, 194-205.

Advances in Cryptology – **ASIACRYPT '91.** Springer-Verlag LNCS 739 (1993).
Editors: H. Imai, R.L. Rivest, and T. Matsumoto.

J. Brandt, I. Damgård, P. Landrock, Speeding up prime number generation, 440–449.

L. Brown, M. Kwan, J. Pieprzyk, J. Seberry, Improving resistance to differential cryptanalysis and the redesign of LOKI, 36-50.

J. Daemen, Limitations of the Even-Mansour construction, 495–498.

J. Daemen, A. Bosselaers, R. Govaerts, J. Vandewalle, Collisions for Schnorr's hash function *FFT-Hash* presented at Crypto'91, 477-480.

J. Daemen, R. Govaerts, J. Vandewalle, A framework for the design of one-way hash functions including cryptanalysis of *Damgård's* one-way function based on a cellular automaton, 82-96.

D.W. Davies, The transition from mechanisms to electronic computers, 1940 to 1950, 1-21.

Y. Desmedt, M. Burmester, An efficient zero-knowledge scheme for the discrete logarithm based on smooth numbers, 360-367.

S. Even, Y. Mansour, A construction of a cipher from a single pseudorandom permutation, 210-224.

J. Feigenbaum, R. Ostrovsky, A note on one-prover, instance-hiding zero-knowledge proof systems, 352–359.

L. Fortnow, M. Szegedy, On the power of two-local random reductions, 346-351.

B. Goldburg, E. Dawson, S. Sridharan, A secure analog speech scrambler using the discrete cosine transform, 299-311.

L. Ham, H.-Y. Lin, An oblivious transferprotocol and its application for the exchange of secrets, 3 12-320.

T. Itoh, K. Sakurai, On the complexity of constant round *ZKIP* of possession of knowledge, 331-345.

T. Itoh, K. Sakurai, H. Shizuya, Any language in *IP* has a divertible ZKIP, 382-396.

A. Joux, J. Stem, Cryptanalysis of another knapsack cryptosystem, 470–476.

T. Kaneko, A known-plaintext attack of FEAL-4 based on the system of linear equations on difference, 485–488.

K. Kim, Construction of DES-like S-boxes based on Boolean functions satisfying the SAC, 59-72.

A. Klapper, M. Goresky, Revealing information with partial period correlations, 277-287.

L.R. Knudsen, Cryptanalysis of LOKI, 22-35.

M. Kwan, Simultaneous attacks in differential cryptanalysis (getting more pairs per encryption), 489–492.

E. Biham, A. Biryukov, How to strengthen DES using existing hardware, 398412.

C. Boyd, W. Mao, Design and analysis of key exchange protocols via secure channel identification, 171–181.

G. Carter, A. Clark, L. Nielsen, *DESV-1:* A variation of the data encryption standard (DES), 427430.

X. Chang, Z.-D. Dai, G. Gong, Some cryptographic properties of exponential functions, 415–418.

C. Chames, J. Pieprzyk, Attacking the SL_2 hashing scheme, 322-330.

S. Chee, S. Lee, K. Kim, Semi-bent functions, 107-118.

A. De Santis, T. Okamoto, G. Persiano, Zero-knowledge proofs of computational power in the shared *string* model, 182-192.

Y. Desmedt, G. Di Crescenzo, M. Burmester, Multiplicative non-abelian sharing schemes and their application to threshold cryptography, 21-32.

A. Fúster-Sabater, P. Caballero-Gil, On the linear complexity of nonlinearly filtered PN-sequences, 80-90.

J.D. Golić, Intrinsic statistical weakness of keystream generators, 91-103.

P. Horster, M. Michels, H. Petersen, Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications, 224-237.

H. Imai, Information security aspects of spread spectrum systems, 193-208.

W.-A. Jackson, K.M. Martin, C.M. O'Keefe, On sharing many secrets, 42-54.

K. Kurosawa, K. Okada, Combinatorial interpretation of secret sharing schemes, 55-64.

K. Kurosawa, K. Okada, K. Sakano, Security of the center in key distribution schemes, 333-341.

K. Kurosawa, K. Okada, S. Tsujii, Low exponent attack against elliptic curve RSA, 376-383.

T. Matsumoto, Incidence structures for key sharing, 342-353.

C.A. Meadows, Formal verification of cryptographic protocols: a survey, 133-150.

M. Mihaljević, A correlation attack on the binary sequence generators with time-varying output function, 67-79.

V. Niemi, A. Renvall, How to prevent buying of votes in computer elections, 164-170.

L. O'Connor, J.D. Golić, A *unified* Markov approach to differential and linear cryptanalysis, 387-397.

K. Okada, K. Kurosawa, Lower bound on the size of shares of nonpertiect secret sharing schemes, 33–41.

J. Patarin, Collisions and inversions for *Damgård's* whole hash function, 307-321.

R. Safavi-Naini, L. Tombak, Combinatorial structure of A-codes with r-fold security, 211-223.

J. Seberry, X.-M. Zhang, Y. Zheng, Structures of cryptographic functions with strong avalanche characteristics, 119-132.

P. Smith, C. Skinner, A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, 357-364.

J. Stem, Can one design a signature scheme based on error-correcting codes?, 424–426.

T. Tokita, T. Sorimachi, M. Matsui, Linear cryptanalysis of LOKI and s^2*DES,* 293-303.

Y. Yacobi, Efficient electronic money, 153-163.

A.2 Crypto Proceedings

ADVANCES IN CRYPTOGRAPHY-A Report on **CRYPTO 81.** ECE Rept No 82-04, Dept. of Electrical & Computer Engineering, University of California, Santa Barbara, CA, U.S.A., 1982. Editor: A. Gersho.

L.M. Adleman, Primality testing (abstract only), 10.

H.R. Amirazizi, M.E. Hellman, Time-memory-processor tradeoffs (abstract only), 7-9.

H.R. Amirazizi, E.D. Kamin, J.M. Reyneri, Compact knapsacks arepolynomiallysolvable (abstract only), 17–19.

H.J. Beker, Stream ciphers: Applications and techniques, 121-123.

T.A. Berson, R.K. Bauer, Local network cryptosystem architecture, 73-78.

G.R. Blakley, Key management from a security viewpoint (abstract only), 82.

M. Blum, Coin Aipping by telephone: A protocol for solving impossible problems, 11-15.

V. Korzhik, V. Yakovlev, Nonasymptotic estimates of information protection efficiency for the wire-tap channel concept, 185-195.

X. Lai, R.A. Rueppel, J. Woollven, A fast cryptographic checksum algorithm based on stream ciphers, 339-348.

C.-S. Laih, S.-M. Yen, Secure addition sequence and its applications on the server-aided secret computation protocols, 219-230.

R. Lidl, W.B. Müller, Primality testing with Lucas functions, 539-542.

C.H. Lim, P.J. Lee, Modified Maurer-Yacobi's scheme and its applications, 308-323.

T. Matsumoto, H. Imai, C.-S. Laih, S.-M. Yen, On verifiable implicit asking protocols for RSA computation, 296-307.

M. Mihaljević, An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure, 349-356.

A. Miyaji, Elliptic curves over F_p suitable for cryptosystems, 479491.

B.B. Nieh, S.E. Tavares, Modelling and analyzing cryptographic protocols using Petri nets, 275-295.

W. Ogata, K. Kurosawa, S. Tsujii, Nonperfect secret sharing schemes, 56-66.

C.M. O'Keefe, A comparison of key distribution patterns constructed from circle geometries, 517-527.

J.C. Paillès, New protocols for electronic money, 263-274.

M. Portz, A generalized description of DES-based and Benes-based permutation generators, 397–409.

B. Preneel, R. Govaerts, J. Vandewalle, An attack on two hash functions by Zheng-Matsumoto-Imai, 535–538.

B. Preneel, R. Govaerts, J. Vandewalle, On the power of memory in the design of collision resistant hash functions, 105-121.

M. Rezny, E. Trimarchi, A block cipher method using combinations of different methods under the control of the user key, 531-534.

R. Safavi-Naini, L. Tombak, Authentication codes under impersonation attack, 35-47.

K. Sakurai, T. Itoh, On bit correlations amongpreimages of "many to one" one-way functions -a new approach to study on randomness and hardness of one-way functions, 435–446.

K. Sakurai, T. Itoh, Subliminal channels for signature transfer and their application to signature distribution schemes, 23 l-243.

T. Satoh, K. Kurosawa, S. Tsujii, Privacy for multi-party protocols, 252-260.

J. Sauerbrey, A modular exponentiation unit based on systolic arrays, 505-5 16.

J. Seberry, X.-M. Zhang, Highly nonlinear O-l balanced Boolean functions satisfying strict avalanche criterion, 145-155.

J. Snare, Information technology security standards – an Australian perspective, 367-384.

L. Tombak, R. Safavi-Naini, Authentication codes with perfect protection, 15-26.

C.P. Waldvogel, J.L. Massey, The probability distribution of the Diffie-Hellman key, 492-504.

J.-H. Yang, Z.-D. Dai, Construction of m-ary de Bruijn sequences, 357-363.

S.-M. Yen, C.-S. Laih, The fast cascade exponentiation algorithm and its applications on cryptography, 447–456.

Y. Zheng, J. Pieprzyk, J. Sebeny, HAV! – a one-way hashing algorithm with variable length of output, 83-104.

E. Zuk, Remarks on "The design of a conference key distribution system", 467468.

Advances in Cryptology – **ASIACRYPT '94.** Springer-Verlag LNCS 917 (1995).
Editors: J. Pieprzyk and R. Safavi-Naini.

M. Abe, H. Morita, Higher radix nonrestoring modular multiplication algorithm and public-key LSI architecture with limited hardware resources, 365-375.

M. Alabbadi, S.B. Wicker, A digital signature scheme based on linear error-correcting block codes, 238-248.

D. Atkins, M. Graff, A.K. Lenstra, PC. Leyland, The magic words are SQUEAMISHOSSIFRAGE, 263-277.

D. Beaver, Factoring: The DNA solution, 419–423.

P. Béguin, J.-J. Quisquater, Secure acceleration of DSS signatures using insecure server, 249-259.

T. Beth, Multifeature security through homomorphic encryption, 1-17.

E. Biham, Cryptanalysis of multiple modes of operation, 278-292.

G. Brassard, On computationally secure authentication tags requiring short secret shared keys, 79-86.

E.F. Brickell, A fast modular multiplication algorithm with applications to two key cryptography, 51-60.

E.F. Brickell, J.A. Davis, G.J. Simmons, A preliminary report on the cryptanalysis of Merkle-Hellman knapsack cryptosystems, 289-301.

E.F. Brickell, J.H. Moore, Some remarks on the Herlestam-Johannesson algorithm for computing logarithms over $GF(2^p)$, 15-19.

D. Chaum, Blind signatures for untraceable payments, 199-203.

D.W. Davies, Some regular properties of the 'Data Encryption Standard' algorithm, 89-96.

D.W. Davies, G.I.P. Parkin, The average cycle size of the key stream in output feedback encipherment, 97-98.

D. Dolev, S. Even, R.M. Karp, On the security ofping-pong protocols, 177-186.

D. Dolev, A. Wigderson, On the security of multi-party protocols in distributed systems, 167-175.

S. Even, 0. Goldreich, On the security of multi-party ping-pong protocols, 315.

S. Even, 0. Goldreich, A. Lempel, A randomized protocol for signing contracts, 205–210.

S. Goldwasser, S. Micali, A. Yao, On signatures and authentication, 211-215.

M.E. Hellman, J.M. Reyneri, Drainage and the DES, 129-l 3 1.

M.E. Hellman, J.M. Reyneri, Fast computation of discrete logarithms in GF(q), 3-13.

R. Janardan, K.B. Lakshmanan, A public-key cryptosystem based on the matrix cover NP-complete problem, 21-37.

R.R. Jueneman, Analysis of certain aspects of output feedback mode, 99-127.

L. Longpré, The use ofpublic-key cryptography for signing checks, 187-197.

M. Merritt, Key reconstruction, 321-322.

C. Mueller-Schloer, N.R. Wagner, Cryptographic protection ofpersonal data cards, 219-229.

C. Nicolai, Nondeterministic cryptography, 323-326.

J.B. Plumstead, *Inferring* a sequence produced by a linear congruence, 3 17-3 19.

R.L. Rivest, A short report on the RSA chip, 327.

R.L. Rivest, A.T. Sherman, Randomized encryption techniques, 145-163.

A. Shamir, A polynomial time *algorithm* for breaking the basic Merkle-Hellman cryptosystem, 279-288.

R.S. Wintemitz, Security of a keystrem cipher with secret initial value, 133-137.

Advances in Cryptology – Proceedings of CRYPTO 83. Plenum Press (1984). Editor: D. Chaum.

S.G. Akl, On the security of compressed encodings, 209-230.

M. Blum, U.V. Vazirani, V.V. Vazirani, Reducibility among protocols, 137-146.

E.F. Brickell, Solving low density knapsacks, 25-37.

E.F. Brickell, J.C. Lagarias, A.M. Odlyzko, Evaluation of the *Adleman* attack on multiply iterated knapsack cryptosystems, 39–42.

D. Chaum, Blind signature system, 153.

D. Chaum, Design concepts for tamper responding systems, 387-392.

D.W. Davies, Use of the 'signature token' to create a negotiable document, 377-382.

M. Davio, Y. Desmedt, M. Fosséprez, R. Govaerts, J. Hulsbosch, P. Neutjens, P. Piret, J.-J. Quisquater, J. Vandewalle, P. Wouters, Analytical characteristics of the DES, 171-202.

J.A. Davis, D.B. Holdridge, Factorization using the quadratic sieve algorithm, 103-113.

D.E. Denning, Field encryption and authentication, 231-247.

T. ElGamal, A subexponential-time algorithm for computing discrete logarithms over $GF(p^2)$, 275–292.

S. Even, 0. Goldreich, Electronic wallet, 383-386.

S. Even, 0. Goldreich, On the power of cascade ciphers, 43-50.

B.W. Fam, Improving the security of exponential key exchange, 359-368.

0. Goldreich, A simple protocol for signing contracts, 133-136.

H. Jiirgensen, D.E. Matthews, Some results on the information theoretic analysis of cryptosystems, 303-356.

J.C. Lagarias, Knapsack public key cryptosystems and diophantine approximation, 3-23.

R. Lidl, W.B. Miiller, Permutation polynomials in RSA-cryptosystems, 293-301.

G. Brassard, An optimally secure relativized cryptosystem, 54-58.

D.L. Chaum, Silo watching, 138-139.

D.W. Davies, Some regular properties of the DES (abstract only), 41.

R.A. DeMillo, N.A. Lynch, M.J. Merritt, The design and analysis of cryptographic protocols (abstract only), 71.

W. Diffie, Cryptographic technology: Fifteen year forecast, 84-108.

S. Even, A protocol for signing contracts, 148-153.

M. Gasser, Limitations of encryption to enforce mandatory security, 130-134.

J.A. Gordon, Towards a design procedure for cryptosecure substitution boxes (abstract only), 53.

M.E. Hellman, E.D. Kamin, J. Reyneri, On the necessity of cryptanalytic exhaustive search, 2-6.

P.S. Henry, R.D. Nash, Fast decryption algorithm for the knapsack cipher (abstract only), 16.

E. Henze, The solution of the general equation for public key distribution systems, 140-141.

T. Herlestam, On the feasibility of computing discrete logarithms using *Adleman's* subexponential algorithm, 142-147.

I. Ingemarsson, Are all injective knapsacks partly solvable after multiplication modulo *q?, 20-24.*

J.P. Jordan, A variant of a public key cryptosystem based on Goppa codes, 25-30.

S.C. Kak, Scrambling and randomization, 59-63.

S.T. Kent, Cryptographic techniques for protecting storage (abstract only), 80.

A.G. Konheim, A one-way sequence for transaction verification (abstract only), 38.

A.L. Lang Jr., J. Vasak, A methodology for evaluating the relative security of commercial COMSEC devices, 124-l 29.

Y.A. Lau, T.R. McPherson, Implementation of a hybrid *RSA/DES* key management system (abstract only), 83.

L.-S. Lee, G.-C. Chou, New results on sampling-based scrambling techniques for secure speech communications, 115-l 19.

H. Meijer, S. Akl, Digital signature schemes, 65-70.

D.R. Morrison, Subtractive encryptors -alternatives to the DES, 42-52.

J.M. Nye, Current market: Products, costs, trends, 110-114.

J.M. Nye, The import/export dilemma (abstract only), 135-137.

S. Porter, A password extension for improved human factors (abstract only), 81.

G. Purdy, G. Simmons, J. Studier, Software protection using "communal-key-cryptosystems" (abstract only), 79.

B.P. Schanning, MEMO: A hybrid approach to encrypted electronic mail (abstract only), 64.

A. Shamir, The generation of cryptographically strong pseudo-random sequences (abstract only), 1.

G.J. Simmons, A system for point-of-sale or access user authentication and identification, 31-37.

M.E. Smid, DES 81: An update, 39–40.

S.B. Weinstein, Security mechanism in electronic cards (abstract only), 109.

A.D. Wyner, Some thoughts on speech encryption (abstract only), 120.

Advances in Cryptology – Proceedings of CRYPTO 82. Plenum Press (1983). Editors: D. Chaum, R.L. Rivest, and A.T. Sherman.

L.M. Adleman, Implementing an electronic notary public, 259-265.

L.M. Adleman, On breaking the iterated *Merkle-Hellman* public-key cryptosystem, 303-308.

S.G. Akl, P.D. Taylor, Cryptographic solution to a multilevel security problem, 237-249.

G.M. Avis, S.E. Tavares, Using data uncertainty to increase the Crypto-complexity of simple private key enciphering schemes, 139-143.

C.H. Bennett, G. Brassard, S. Breidbart, S. Wiesner, Quantum cryptography, or unforgeable subway tokens, 267-275.

T.A. Berson, Local network cryptosystem architecture: Access control, 251-258.

T.A. Berson, *Long key* variants *of DES,* 311-313.

G.R. Blakley, L. Swanson, Infinite structures in information theory, 39-50.

R. Blom, Non-public key distribution, 231-236.

L. Blum, M. Blum, M. Shub, Comparison of two pseudo-random number generators, 61-78.

J.A. Reeds, J.L. Manferdelli, DES has no per round linear factors, 377-389.
SC. Serpell, C.B. Brookson, B.L. Clark, A prototype encryption system using public key, 3-9.
A. Shamir, Identity-based cryptosystems and signature schemes, 47-53.
G.J. Simmons, Authentication theory/coding theory, 41 1–43 1.
T. Tedrick, Fair exchange of secrets, 434-438.
U.V. Vazirani, V.V. Vazirani, Efficient and secure pseudo-random number generation, 193-202.
N.R. Wagner, M.R. Magyarik, A public key cryptosystem based on the word problem, 19-36.
H.C. Williams, Some public key Crypto-functions as intractable as factorization, 66-70.
M. Yung, Cryptoprotocols: Subscription to a public key, the secret blocking and the multi-player mental poker game, 439–453.

Advances in Cryptology – CRYPTO '85. Springer-Verlag LNCS 218 (1986).
Editor: H.C. Williams.

C.H. Bennett, G. Brassard, J.-M. Robert, How to reduce your enemy's information, 468–476.
R. Berger, S. Kannan, R. Peralta, A framework for the study of cryptographic protocols, 87-103.
G.R. Blakley, Information theory without the finiteness assumption, II. Unfolding the DES, 282-337.
G.R. Blakley, C. Meadows, G.B. Purdy, Fingerprinting long forgiving messages, 180-189.
E.F. Brickell, J.M. DeLaurentis, An attack on a signature schemeproposed by Okamoto and Shiraishi, 28-32.
D. Chaum, J.-H. Evertse, Cryptanalysis of DES with a reduced number of rounds -sequences of linear factors in block ciphers, 192-211.
B. Chor, 0. Goldreich, S. Goldwasser, The bit security of modular squaring given partial factorization of the modulos, 448–457.
D. Coppersmith, Another birthday attack, 14-17.
D. Coppersmith, Cheating at mental poker, 104-107.
D. Coppersmith, The real reason for Rivest's phenomenon, 535-536.
C. Crépeau, A secure poker protocol that minimizes the effect of player coalitions, 73-86.
W. de Jonge, D. Chaum, Attacks on some RSA signatures, 18-27.
Y. Desmedt, Unconditionally secure authentication schemes and practical and theoretical consequences, 42-55.
Y. Desmedt, A.M. Odlyzko, A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes, 5 16-522.
W. Diffie, Security for the DoD transmission control protocol, 108-127.
T. ElGamal, On computing logarithms over finite fields, 396–402.
D. Estes, L.M. Adleman, K. Kompella, K.S. McCurley, G.L. Miller, Breaking the Ong-Schnorr-Shamir signature scheme for quadratic number fields, 3-13.
S. Even, 0. Goldreich, A. Shamir, On the security of ping-pong protocols when implemented using the RSA, 58-72.
J. Feigenbaum, Encryptingproblem instances: Or. . . , can you take advantage of someone without having to trust him?, 477–488.
H. Fell, W. Diffie, Analysis of a public key approach based on polynomial substitution, 340-349.
Z. Galil, S. Haber, M. Yung, Symmetric public-key encryption, 128-137.
P. Godlewski, G.D. Cohen, Some cryptographic aspects of Womcodes, 458–467.
J.R. Gosler, Software protection: Myth or reality?, 140-157.
J. Håstad, On using RSA with low exponent in a public key network, 403-408.
W. Haemers, Access control at the Netherlands Postal and Telecommunications Services, 543-544.
A. Herzberg, S. Pinter, Public protection of software, 158-179.
B.S. Kaliski Jr., R.L. Rivest, A.T. Sherman, Is DES a pure cipher? (Results of more cycling experiments on DES), 2 12-226.
M. Kochanski, Developing an RSA chip, 350-357.
M. Luby, C. Rackoff, How to construct pseudo-random permutations from pseudo-random functions, 447.
VS. Miller, Use of elliptic curves in cryptography, 417426.
T.E. Moore, S.E. Tavares, A layered approach to the design of private key cryptosystems, 227-245.
E. Okamoto, K. Nakamura, Lifetimes of keys in cryptographic key management systems, 246-259.

H. Ong, C.P. Schnorr, Signatures through approximate *respresentations* by quadratic forms, 117-l 3 1.

C. Pomerance, J.W. Smith, S.S. Wagstaff Jr., New ideas for factoring large integers, 81-85.

J.A. Reeds, N.J.A. Sloane, Shift-register synthesis (modulo m), 249.

J.E. Sachs, S. Berkovits, Probabilistic analysis andperformance modelling of the 'Swedish' *algorithm and* modifications, 253-273.

G.J. Simmons, The prisoners' problem and the subliminal channel, 51-67.

M.E. Spencer, S.E. Tavares, A layered *broadcaset* cryptographic system, 157-170.

T. Tedrick, How to exchange half a bit, 147-151.

U.V. Vazirani, V.V. Vazirani, RSA bits are $.732 + \epsilon$ secure, 369-375.

H.C. Williams, An overview of factoring, 71-80.

R.S. Wintemitz, Producing a one-way hash function from DES, 203-207.

M.C. Wunderlich, Factoring numbers on the massively parallel computer, 87-102.

Advances in Cryptology – Proceedings of CRYPTO 84. Springer-Verlag LNCS 196 (1985). Editors: G.R. Blakley and D. Chaum.

S.G. Akl, H. Meijer, A fast pseudo random permutation generator with applications to cryptology, 269-275.

H. Beker, M. Walker, Key management for secure electronic funds transfer in a retail environment, 401-410.

C.H. Bennett, G. Brassard, An update on quantum cryptography, 475480.

I.F. Blake, R.C. Mullin, S.A. Vanstone, Computing logarithms in $GF(2^n)$, 73-82.

G.R. Blakley, Information theory without the finiteness assumption, *I:* Cryptosystems as group-theoretic objects, 314–338.

G.R. Blakley, C. Meadows, Security of ramp schemes, 242-268.

M. Blum, S. Goldwasser, An efficient probabilistic public-key encryption scheme which hides all partial information, 289-299.

E.F. Brickell, Breaking iterated knapsacks, 342-358.

D. Chaum, How to keep a secret alive: Extensible partial key, key safeguarding, and threshold systems, 48 1–485.

D. Chaum, New secret codes can prevent a computerized big brother, 432433.

S.-S. Chen, On rotation group and encryption of analog signals, 95-100.

B. Chor, 0. Goldreich, *RSA/Rabin* least significant bits are $1/2 + 1/poly(\log n)$ secure, 303-313.

B. Chor, R.L. Rivest, A knapsack type public key cryptosystem based on arithmetic in finite fields, 54-65.

D.W. Davies, A message authenticator algorithm suitable for a mainframe computer, 393–400.

M. Davio, Y. Desmedt, J. Goubert, F. Hoomaert, J.-J. Quisquater, Efficient hardware and software implementations for the DES, 144-146.

J.A. Davis, D.B. Holdridge, An update on factorization at Sandia National Laboratories, 114.

Y. Desmedt, J.-J. Quisquater, M. Davio, Dependence of output on input in DES: Small avalanche characteristics, 359-376.

T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, 10-18.

R.C. Fairfield, A. Matusevich, J. Plany, An *LSI* digital encryption processor *(DEP),* 115-143.

R.C. Fairfield, R.L. Mortenson, K.B. Coulthart, An *LSI* random number generator *(RNG),* 203-230.

S. Fortune, M. Merritt, Poker protocols, 454-464.

0. Goldreich, S. Goldwasser, S. Micali, On the cryptographic applications *of random* functions, 276-288.

S. Goldwasser, S. Micali, R.L. Rivest, A "paradoxical" solution to the signature problem, 467.

F. Hoomaert, J. Goubert, Y. Desmedt, Efficient hardware implementation of the DES, 147-173.

B.S. Kaliski, *Wyner's* analog encryption scheme: Results of a simulation, 83-94.

A.G. Konheim, Cryptanalysis *of ADFGVX encipherment* systems, 339-341.

S.C. Kothari, Generalized linear threshold scheme, 231-241.

A.C. Leighton, S.M. Matyas, The history of book ciphers, 101-113.

A.K. Leung, S.E. Tavares, Sequence complexity as a test for cryptographic systems, 468-474.

H. Ong, C.P. Schnorr, A. Shamir, Efficient signature schemes based on polynomial equations, 37-46.

N. Proctor, A self-synchronizing cascaded cipher system with dynamic control of error propagation, 174–190.

S. Micali, C. Rackoff, B. Sloan, The notion of security forprobabilistic cryptosystems, 381-392.

J.H. Moore, G.J. Simmons, Cycle structure of the DES with weak and semi-weak keys, 9-32.

G.A. Orton, M.P. Roy, P.A. Scott, L.E. Peppard, S.E. Tavares, VLSI implementation of public-key encryption algorithms, 277-301.

G. Ranlcine, THOMAS - a complete single chip RSA device, 480-487.

T.R.N. Rao, K.-H. Nam, Private-key algebraic-coded cryptosystems, 35–48.

D.R. Stinson, Some constructions and bounds for authentication codes, 418-425.

M. Tompa, H. Woll, How to share a secret with cheaters, 261-265.

N.R. Wagner, P.S. Putter, M.R. Cain, Large-scale randomization techniques, 393404.

Advances in Cryptology – **CRYPTO** '87. Springer-Verlag LNCS 293 (1988).
Editor: C. Pomerance.

C.M. Adams, H. Meijer, Security-related comments regarding McEliece's public-key cryptosystem, 224–228.

P. Beauchemin, G. Brassard, A generalization of Hellman's extension of Shannon's approach to cryptography, 46 1.

G.R. Blakley, W. Rundell, Cryptosystems based on an analog of heat *flow,* 306-329.

E.F. Brickell, D. Chaum, I.B. Damgård, J. van de Graaf, Gradual and verifiable release of a secret, 156-166.

E.F. Brickell, P.J. Lee, Y. Yacobi, Secure audio teleconference, 418-426.

D. Chaum, C. Crépeau, I. Damgård, Multiparty unconditionally secure protocols, 462.

D. Chaum, I.B. Damgård, J. van de Graaf, Multiparty computations ensuring privacy of each party's input and correctness of the result, 87-l 19.

C. Crépeau, Equivalence between two Aavours of oblivious transfers, 350-354.

G.I. Davida, F.B. Dancs, A Crypto-engine, 257-268.

G.I. Davida, B.J. Matt, Arbitration in tamper proof systems (If DES $\approx$ RSA then what's the difference between true signature and arbitrated signature schemes?), 216-222.

A. De Santis, S. Micali, G. Persiano, Non-interactive zero-knowledge proof systems, 52-72.

J.M. DeLaurentis, Components and cycles of a random function, 231-242.

Y. Desmedt, Society and group oriented cryptography: A new concept, 120–127.

Y. Desmedt, C. Goutier, S. Bengio, Special uses and abuses of the Fiat-Shamirpassport protocol, 21-39.

EA. Feldman, Fast spectral tests for measuring nonrandomness and the DES, 243-254.

W. Fumy, On the F-function of FEAL, 434-437.

Z. Galil, S. Haber, M. Yung, Cryptographic computation: Secure fault-tolerant protocols and the *public*-key model, 135-155.

0. Goldreich, R. Vainish, How to solve any protocol problem - an efficient improvement, 73-86.

L. Guillou, J.-J. Quisquater, Efficient digital public-key signatures with shadow, 223.

M.P. Herlihy, J.D. Tygar, How to make replicated data secure, 379-391.

R. Impagliazzo, M. Yung, Direct minimum-knowledge computations, 40-5 1.

R.A. Kemmerer, Analyzing encryption protocols using formal verification techniques, 289-305.

K. Koyama, K. Ohta, Identity-based conference key distribution systems, 175-184.

M. Luby, C. Rackoff, A study ofpassword security, 392-397.

Y. Matias, A. Shamir, A video scrambling technique based on space filling curves, 398–417.

T. Matsumoto, H. Imai, On the keypredistribution system: A practical solution to the key distribution problem, 185-193.

R.C. Merkle, A digital signature based on a conventional encryption function, 369-378.

J.H. Moore, Strong practical protocols, 167-172.

E. Okamoto, Key distribution systems based on identification information, 194-202.

K. Presttun, Integrating cryptography in ISDN, 9-18.

W.L. Price, Standards for data security – a change of direction, 3-8.

J.-J. Quisquater, Secret distribution of keys for public-key systems, 203-208.

J.-J. Quisquater, J.-P. Delescaille, Other cycling tests for DES, 255-256.

T.R.N. Rao, On Struik-Tilburg cryptanalysis of Rao-Nam scheme, 458-460.

J.-J. Quisquater, Y. Desmedt, M. Davio, The importance of "good" key scheduling schemes (how to make a secure DES scheme with $\leq$ 48 bit keys?), 537-542.

J.H. Reif, J.D. Tygar, Efficient parallel pseudo-random number generation, 433–446.

R.A. Rueppel, Correlation immunity and the summation generator, 260-272.

A. Shamir, On the security of DES, 280-281.

T. Siegenthaler, Design of combiners to prevent divide and conquer attacks, 273-279.

G.J. Simmons, A secure subliminal channel (?), 33–41.

N.M. Stephens, Lenstra's factorisation method based on elliptic curves, 409416.

J. van Tilburg, D.E. Boekee, Divergence bounds on key equivocation and error probability in cryptanalysis, 489-5 13.

V. Varadharajan, Trapdoor rings and their use in cryptography, 369-395.

A.F. Webster, S.E. Tavares, On the design of S-boxes, 523-534.

H.C. Williams, An M^3 public-key encryption scheme, 358-368.

S. Wolfram, Cryptography with cellular automata, 429432.

Advances in Cryptology – CRYPTO '86. Springer-Verlag LNCS 263 (1987). Editor: A.M. Odlyzko.

P. Barrett, Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor, 3 1 l-323.

P. Beauchemin, G. Brassard, C. Crepeau, C. Goutier, Two observations on probabilistic primality testing, 443–450.

J.C. Benaloh, Cryptographic capsules: A disjunctive primitive for interactive protocols, 213-222.

J.C. Benaloh, Secret sharing homomorphisms: Keeping shares of a secret secret, 251-260.

T. Beth, B.M. Cook, D. Gollmann, Architectures for exponentiation in $GF(2^n)$, 302-310.

G.R. Blakley, R.D. Dixon, Smallest possible message expansion in threshold schemes, 266-274.

G. Brassard, C. Crépeau, Zero-knowledge simulation of Boolean circuits, 223-233.

G. Brassard, C. Crepeau, J.-M. Robert, All-or-nothing disclosure of secrets, 234-238.

E.F. Brickell, J.H. Moore, M.R. Purtill, Structure in the S-boxes of the DES, 3-8.

J.J. Cade, A modification of a broken public-key cipher, 64–83.

A.H. Chan, R.A. Games, On the linear span of binary sequences obtained from finite geometries, 405417.

D. Chaum, Demonstrating that a public predicate can be satisfied without revealing any information about bow, 195-199.

D. Chaum, J.-H. Evertse, A secure and privacy-protecting protocol for transmitting personal information between organizations, 118-l 67.

D. Chaum, J.-H. Evertse, J. van de Graaf, R. Peralta, Demonstrating possession of a discrete logarithm without revealing it, 200–212.

C. Crepeau, A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face, 239-247.

W. de Jonge, D. Chaum, Some variations on RSA signatures and their security, 49-59.

Y. Desmedt, Is there an ultimate use of cryptography?, 459-463.

Y. Desmedt, J.-J. Quisquater, Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?), 111-117.

A. Fiat, A. Shamir, How to prove yourself: Practical solutions to identification and signature problems, 186-194.

0. Goldreich, Towards a theory of software protection, 426–439.

0. Goldreich, Two remarks concerning the Goldwasser-Micali-Rivest signature scheme, 104-l 10.

0. Goldreich, S. Micali, A. Wigderson, How to prove all NP statements in zero-knowledge, and a methodology of cryptographic protocol design, 171-185.

L.C. Guillou, M. Ugon, Smart card – a highly reliable and portable security device, 464-479.

R. Gyoery, J. Seberry, Electronic funds transfer point of sale in Australia, 347-377.

N.S. James, R. Lidl, H. Nieclerreiter, Breaking the Cade cipher, 60-63.

R.R. Jueneman, A high speed manipulation detection code, 327-346.

B.S. Kaliski Jr., A pseudo-random bit generator based on elliptic logarithms, 84–103.

S.M. Matyas, Public-key registration, 451-458.

Prev. Chapter Prev. Page Home Next Page

M. Lucks, A constraint satisfaction algorithm for the automated decryption of simple substitution ciphers, 132-144.

T. Matsumoto, K. Kato, H. Imai, Speeding up secret computations with insecure auxiliary devices, 497-506.

S. Micali, C.P. Schnorr, Efficient, perfect random numbergenerators, 173-198.

S. Micali, A. Shamir, An improvement of the Fiat-Shamir identification and signature scheme, 244-247.

K. Ohta, T. Okamoto, A modification of the Fiat-Shamir scheme, 232-243.

C. Rackoff, A basic theory *of public* and private cryptosystems, 249-255.

J.R. Sherwood, V.A. Gallo, The application of smart cards for RSA digital signatures in a network comprising both interactive and store-and-forward facilities, 484-496.

G.J. Simmons, How to (really) share a secret, 390-448.

D.G. Steer, L. Strawczynski, W. Diffie, M. Wiener, A secure audio teleconference system, 520-528.

J. van Tilburg, On the McEliece public-key cryptosystem, 119-l 3 1.

K. Zeng, M. Huang, On the linear syndrome method in cryptanalysis, 469478.

Advances in Cryptology – **CRYPTO ‘89.** Springer-Verlag LNCS 435 (1990).
Editor: G. Brassard.

C. Adams, S. Tavares, Good S-boxes are easy to *find,* 612-615.

P. Barrett, R. Eisele, The smart diskette – a universal user token and personal Crypto-engine, 74-79.

D. Beaver, Multiparty protocols tolerating half faulty processors, 560-572.

D. Beaver, S. Goldwasser, Multiparty computation with faulty majority, 589-590.

M. Bellare, L. Cowen, S. Goldwasser, On the structure of secret key exchange protocols, 604-605.

M. Bellare, S. Goldwasser, Newparadigms for digital signatures and message authentication based on *non*-interactive zero knowledge proofs, 194–211.

M. Bellare, S. Micali, Non-interactive oblivious transfer and applications, 547-557.

M. Ben-Or, S. Goldwasser, J. Kilian, A. Wigderson, Efficient identification schemes using two prover interactive proofs, 498-506.

A. Bender, G. Castagnoli, On the implementation of elliptic curve cryptosystems, 186-192.

J. Bos, M. Coster, Additon chain heuristics, 400-407.

J. Boyar, R. Peralta, On the concrete complexity of zero-knowledge proofs, 507-525.

R.L. Brand, Problems with the normal use of cryptography for providing security on unclassified networks, 30–34

E.F. Brickell, A survey of hardware implementations of RSA, 368-370.

E.F. Brickell, D.M. Davenport, On the classification of ideal secret sharing schemes, 278-285.

J.A. Buchmann, H.C. Williams, A key exchange system based on real quadratic fields, 335-343.

A.H. Chan, R.A. Games, On the quadratic spans ofperiodic sequences, 82-89.

D. Chaum, The Spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities, 591-602.

D. Chaum, H. van Antwerpen, Undeniable signatures, 212-216.

G.C. Chick, S.E. Tavares, Flexible access control with master keys, 316-322.

B. Chor, E. Kushilevitz, Secret sharing over infinite domains, 299-306.

R. Cleve, Controlled gradual disclosure schemes for random bits and their applications, 573-588.

I.B. Damgård, A design principle for hash functions, 416-427.

I.B. Damgård, On the existence of bit commitment schemes and zero-knowledge proofs, 17-27.

M. De Soete, J.-J. Quisquater, K. Vedder, A signature with shared verification scheme, 253-262.

Y.G. Desmedt, Making conditionally secure cryptosystems unconditionally abuse-free in a general context, 6-16.

Y.G. Desmedt, Y. Frankel, Threshold cryptosystems, 307-315.

S. Even, 0. Goldreich, S. Micali, On-line/off-line digital signatures, 263-275.

U. Feige, A. Shamir, Zero knowledge proofs of knowledge in two rounds, 526–544.

D.C. Feldmeier, P.R. Kam, *UNIX password* security – ten years later, 4463.

A. Fiat, Batch RSA, 175-185.

P.A. Findlay, B.A. Johnson, Modular exponentiation using recursive sums of residues, 371-386.

G.J. Simmons, An impersonation-proof identity verification scheme, 211-215.

G.J. Simmons, A natural taxonomy for digital information authentication schemes, 269-288.

D.R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, 355-366.

D.R. Stinson, S.A. Vanstone, A combinatorial approach to threshold schemes, 330-339.

R. Struik, J. van Tilburg, The Rao-Nam scheme is insecure against a chosen-plaintext attack, 445–457.

H. Tanaka, A realization scheme for the identity-based cryptosystem, 340-349.

J. van de Graaf, R. Peralta, A simple and secure way to show the validity ofyourpublic key, 128-134.

Y. Yacobi, Attack on the Koyama-Ohta identity based key distribution scheme, 429433.

K.C. Zeng, J.H. Yang, Z.T. Dai, Patterns of entropy drop of the key in an S-box of the DES, 438-444.

Advances in Cryptology – CRYPTO '88. Springer-Verlag LNCS 403 (1990). Editor: S. Goldwasser.

M. Abadi, E. Allender, A. Broder, J. Feigenbaum, L.A Hemachandra, On generating solved instances of computational problems, 297-310.

L.M. Adleman, An abstract theory of computer viruses, 354-374.

E. Bach, Intractable problems in number theory, 77-93.

M. Bellare, S. Micali, How to sign given any trapdoor function, 200-215.

M. Ben-Or, 0. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali, P. Rogaway, Everything provable is provable in zero-knowledge, 37-56.

J. Benaloh, J. Leichter, Generalized secret sharing and monotone functions, 27-35.

M. Blum, P. Feldman, S. Micali, Proving security against chosen ciphertext attacks, 256-268.

J. Brandt, I.B. Damgård, P. Landrock, T. Pedersen, Zero-knowledge authentication scheme with secret key exchange, 583-588.

G. Brassard, I.B. Damgård, “Practical *IP*” $\subseteq$ MA, 580-582.

E.F. Brickell, D.R. Stinson, The detection of cheaters in threshold schemes, 564-577.

D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, 319-327.

C. Crépeau, J. Kilian, Weakening security assumptions and oblivious transfer, 2-7.

I.B. Damglrd, On the randomness of Legendre and Jacobi sequences, 163-172.

I.B. Damgård, Payment systems and credential mechanisms with provable security against abuse by individuals, 328-335.

A. De Santis, S. Micali, G. Persiano, Non-interactive zero-knowledge with preprocessing, 269-282.

M. De Soete, Bounds and constructions for authentication-secrecy codes with splitting, 311-317.

B. den Boer, Diffie-Hellman is as strong as discrete log for certain primes, 530-539.

Y. Desmedt, Abuses in cryptography and how to tight them, 375-389.

C. Dwork, L. Stockmeyer, Zero-knowledge with finite state verifiers, 71-75.

U. Feige, A. Shamir, M. Tennenholtz, The noisy oracle problem, 284–296.

R. Forré, The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition, 450–468.

M. Girault, P. Toffin, B. Vallée, Computation of approximate L-th roots modulo n and application to cryptography, 100-l 17.

0. Goldreich, H. Krawczyk, M. Luby, On the existence ofpseudorandom generators, 146-162.

0. Goldreich, E. Kushilevitz, A perfect zero-knowledge proof for a problem equivalent to discrete logarithm, 57-70.

L.C. Guillou, J.-J. Quisquater, A “paradoxical” identity-based signature scheme resulting from zero-knowledge, 216-231.

B.J. Herbison, Developing Ethernet enhanced-security system, 507-519.

M.-D.A. Huang, S.-H. Teng, A universal problem in secure and verifiable distributed computation, 336-352.

T. Hwang, T.R.N. Rao, Secret error-correcting codes *(SECC)*, 540–563.

R. Impagliazzo, S. Rudich, Limits on the provable consequences of one-way permutations, 8-26.

N. Koblitz, A family of Jacobians suitable for discrete log cryptosystems, 94-99.

S.A. Kurtz, S.R. Mahaney, J.S. Royer, On the power of l-way functions, 578-579.

R.T.C. Kwok, M. Beale, Aperiodic linear complexities of de Bruijn sequences, 479482.

T.W. Cusick, M.C. Wood, The REDOC II cryptosystem, 545-563.

A. De Santis, M. Yung, Cryptographic applications of the non-interactive metaproof and many-prover systems, 366-377.

D. de Waleffe, J.-J. Quisquater, CORSAIR: A smart card forpublic key cryptosystems, 502-513.

Y. Desmedt, M. Yung, Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks, 177-188.

S. Even, Systolic modular multiplication, 619-624.

W. Fumy, M. Munzert, A modular approach to key distribution, 274-283.

H. Gilbert, G. Chasst, A statistical attack of the Feal-8 cryptosystem, 22-33.

S. Goldwasser, L. Levin, Fair computation of general functions in presence of immoral majority, 77-93.

S. Haber, W.S. Stornetta, How to time-stamp a digital document, 437–455.

J. Kilian, Achieving zero-knowledge robustly, 313-325.

J. Kilian, Interactive proofs with provable security against honest verifiers, 378-392.

K. Kim, T. Matsumoto, H. Imai, A recursive construction method of S-boxes satisfying strict avalanche criterion, 564-574.

N. Koblitz, Constructing elliptic curve cryptosystems in characteristic 2, 156-167.

K. Kompella, L. Adleman, Fast checkers for cryptography, 5 15-529.

K. Koyama, R. Terada, Nonlinear parity circuits and their cryptographic applications, 582-600.

K. Kurosawa, S. Tsujii, Multi-language zero knowledge interactive proof systems, 339-352.

B.A. LaMacchia, A.M. Odlyzko, Computation of discrete logarithms in prime fields, 616-618.

B.A. LaMacchia, A.M. Odlyzko, Solving large sparse linear systems over finite fields, 109-133.

D. Lapidot, A. Shamir, Publicly verifiable non-interactive zero-knowledge proofs, 353-365.

U.M. Maurer, A universal statistical test for random bit generators, 409–420.

J.L. McInnes, B. Pinkas, On the impossibility ofprivate key cryptography with weakly random keys, 421-435.

R.C. Merkle, Fast software encryption functions, 476-501.

S. Micali, T. Rabin, Collective coin tossing without assumptions nor broadcasting, 253-266.

S. Miyaguchi, The FEAL, cipher family, 627-638.

T. Okamoto, K. Ohta, How to utilize the randomness of zero-knowledge proofs, 456–475.

R.L. Rivest, Finding four million large random primes, 625-626.

R.L. Rivest, The MD4 message digest algorithm, 303-311.

A.W. Schrift, A, Shamir, On the universality of the next bit test, 394–408.

G.J. Simmons, Geometric shared secret and/or shared control schemes, 216-241.

0. Staffelbach, W. Meier, Cryptographic significance of the carry for ciphers based on integer addition, 601-614.

P. van Oorschot, A comparison of practical public-key cryptosystems based on integer factorization and discrete logarithms, 576-58 1.

Y. Yacobi, Discrete-log with compressible exponents, 639-643.

Y. Yacobi, A key distribution "paradox", 268-273.

K. Zeng, C.H. Yang, T.R.N. Rao, An improved linear syndrome algorithm in cryptanalysis with applications, 34-47.

Y. Zheng, T. Matsumoto, H. Imai, Structural properties of one-way hash functions, 285-302.

Advances in Cryptology – **CRYPTO '91.** Springer-Verlag LNCS 576 (1992).
Editor: J. Feigenbaum.

M. Abadi, M. Burrows, B. Lampson, G. Plotkin, A calculus for access control in distributed systems, 1–23.

D. Beaver, Efficient multiparty protocols using circuit randomization, 420-432.

D. Beaver, Foundations of secure interactive computing, 377-391.

C.H. Bennett, G. Brassard, C. Crépeau, M.-H. Skubiszewska, Practical quantum oblivious transfer, 351–366.

E. Biham, A. Shamir, Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI, and Lucifer, 156-171.

0. Goldreich, H. Krawczyk, Sparsepseudorandom distributions, 113-127.

C.J.A. Jansen, D.E. Boekee, The shortest feedback shift register that can generate a given sequence, 90-99.

D. Kahn, Keying the German navy's Enigma, 2-5.

J. Kilian, S. Micali, R. Ostrovsky, Minimum resource zero-knowledge proofs, 545-546.

J.T. Kohl, The use of encryption in Kerberos for network authentication, 35–43.

H. Krawczyk, How to predict *congruential* generators, 138-153.

C.-S. Laih, L. Ham, J.-Y. Lee, T. Hwang, Dynamic threshold scheme based on the definition of *cross*-product in an n-dimensional linear space, 286-298.

S.S. Magliveras, N.D. Memon, Properties of cryptosystem PGM, 447–460.

U.M. Maurer, J.L. Massey, Perfect local randomness in pseudo-random sequences, 100–1 12.

R.C. Merkle, A certified digital signature, 218-238.

R.C. Merkle, One way hash functions and DES, 428-446.

S. Miyaguchi, The FEAL - 8 cryptosystem and a call for attack, 624-627.

H. Morita, A fast modular-multiplication algorithm based on a higher radix, 387-399.

M. Naor, Bit commitment using pseudo-randomness, 128-l 36.

R. Nelson, J. Heimann, SDNS architecture and end-to-end encryption, 356-366.

T. Okamoto, K. Ohta, Disposable zero-knowledge authentications and their applications to untraceable electronic cash, 481–496.

R. Ostrovsky, An efficient software protection scheme, 610-611.

B. Preneel, A. Bosselaers, R. Govaerts, J. Vandewalle, A chosen text attack on the modified cryptographic checksum algorithm of Cohen and Huang, 154-l 63.

W.L. Price, Progress in data security *standardisation,* 620–623.

J.-J. Quisquater, J.-P. Delescallle, How easy is collision search. New results *and* applications to DES, 408-413.

J.-J. Quisquater, L. Guillou, T. Berson, How to explain zero-knowledge protocols to your children, 628–631.

C.P. Schnorr, Efficient identification and signatures for smart cards, 239-252.

A. Shamir, An efficient identification scheme based on permuted kernels, 606-609.

J.M. Smith, Practical problems with a cryptographic protection scheme, 64–73.

M. Tatebayashi, N. Matsuzalci, D.B. Newman Jr., Key distribution protocol for digital mobile communication systems, 324-334.

S.R. White, Covert distributed processing with computer viruses, 616-619.

Y. Yacobi, Z. Shmuely, On key distribution systems, 344-355.

K. Zeng, C.H. Yang, T.R.N. Rao, On the linear consistency test (LCT) in cryptanalysis with applications, 164-174.

Y. Zheng, T. Matsumoto, H. Imai, On the construction of block ciphers provably secure and not relying on any unproved hypotheses, 461480.

Advances in Cryptology – CRYPTO '90. Springer-Verlag LNCS 537 (1991). Editors: A.J. Menezes and S.A. Vanstone.

D. Beaver, J. Feigenbaum, J. Kilian, P. Rogaway, Security with low communication overhead, 62-76.

D. Beaver, J. Feigenbaum, V. Shoup, Hiding instances in zero-knowledge proof systems, 326-338.

T. Beth, Y. Desmedt, Identification tokens – or: Solving the chess grandmasterproblem, 169-176.

E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, 2-21.

J. Boyar, D. Chaum, I.B. Damgård, T. Pedersen, Convertible undeniable signatures, 189-205.

G. Brassard, C. Crépeau, Quantum bit commitment and coin tossing protocols, 49-61.

G. Brassard, M. Yung, One-way group actions, 94-107.

E.F. Brickell, D.R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, 242-252.

J. Buchmann, S. Düllmann, On the computation of discrete logarithms in class groups, 134-139.

D. Chaum, S. Roijakkers, Unconditionally-secure digital signatures, 206-214.

C.-C. Chuang, J.G. Dunham, Matrix extensions of the RSA algorithm, 140-155.

R. Cleve, Complexity theoretic issues concerning block ciphers related to D.E.S., 530–544.

J.N.E. Bos, D. Chaum, Provably *unforgeable* signatures, 1-14.

J. Brandt, I. Damgård, On generation ofprobable primes by incremental search, 358-370.

K.W. Campbell, M.J. Wiener, DES is not a group, 512-520.

C. Carlet, Partially-bent functions, 280-291.

D. Chaum, T.P. Pedersen, *Wallet* databases with observers, 89–105.

C. Dwork, U. Feige, J. Kilian, M. Naor, M. Safra, Low communication Z-prover zero-knowledge proofs for NP, 215-227.

C. Dwork, M. Naor, Pricing via processing or combatting junk mail, 139-147.

H. Eberle, A high-speed DES implementation for network applications, 521-539.

M. Fellows, N. Koblitz, Kid *krypto,* 371-389.

Y. Frankel, Y. Desmedt, M. Burrnester, Non-existence of homomorphic general sharing schemes for some key spaces, 549-557.

S. Goldwasser, R. Ostrovsky, Invariant signatures and non-interactive zero-knowledge proofs are equivalent, 228-245.

D.M. Gordon, Designing and detecting trapdoors for discrete Jog cryptosystems, 66-75.

D.M. Gordon, K.S. McCurley, Massively parallel computations of discrete logarithms, 312-323.

L. Harn, H.-Y. Lin, An l-span generalized secret sharing scheme, 558-565.

A. Herzberg, M. Luby, Public randomness in cryptography, 421–432.

R. Hirschfeld, *Making* electronic refunds safer, 106-l 12.

L.R. Knudsen, Iterative characteristics of DES and s^2-*DES,* 497-511.

K. Koyama, Y. Tsuruoka, Speeding up elliptic cryptosystems by using a signed binary window method, 345-357.

U.M. Maurer, Protocols for secret key agreement by public discussion based on common information, 461–470.

W. Meier, 0. Staffelbach, Efficient multiplication on certain *nonsupersingular* elliptic curves, 333-344.

S. Micali, Fairpublic-key cryptosystems, 113-138.

M. Naor, R. Ostrovsky, R. Venkatesan, M. Yung, Perfect zero-knowledge arguments for NP can be based on general complexity assumptions, 196-214.

K. Nyberg, L.R. Knudsen, Provable security against differential cryptanalysis, 566-574.

T. Okamoto, Provably secure and practical identification schemes and corresponding signature schemes, 31-53.

T. Okamoto, A. Fujioka, E. Fujisaki, An efficient digital signature scheme based on an elliptic curve over the ring Z_n , 54-65.

R. Peralta, A quadratic sieve on the n-dimensional cube, 324-332.

A. Russell, Necessary and sufficient conditions for collision-free hashing, 433–441.

K. Sakurai, T. Itoh, On the discrepancy between serial *and parallel* ofzero-knowledge protocols, 246-259.

M. Sivabalan, S. Tavares, L.E. Peppard, On the design of *SP networks* from an information theoretic point of view, 260-279.

M.E. Smid, D.K. Branstad, Response to comments on the *NIST proposed* digital signature standard, 76-88.

D.R. Stinson, New general lower bounds on the information rate of secret sharing schemes, 168-182.

E. van Heijst, T.P. Pedersen, B. Pfitzmann, New constructions of fail-stop signatures and lower bounds, 15-30.

S. Vaudenay, *FFT-Hash-II is* not yet collision-free, 587-593.

P.C. Wayner, Content-addressable search engines and DES-like systems, 575-586.

Y. Zheng, J. Seberry, Practical approaches to attaining security against adaptively chosen ciphertext attacks, 292-304.

R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, Systematic design of two-party authentication protocols, 44-61.

A.G. Broscius, J.M. Smith, Exploiting parallelism in hardware implementation of the DES, 367-376.

P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation-immune functions, 86-100.

R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro, On the size of shares for secret sharing schemes, 101-113.

D. Chaum, E. van Heijst, B. Pfitzmann, Cryptographically strong undeniable signatures, unconditionally secure for the signer, 470-484.

Y.M. Chee, A. Joux, J. Stem, The cryptanalysis of a new public-key cryptosystem based on modular knapsacks, 204–2 12.

I.B. Damgård, Towards practical public key systems secure against chosen ciphertext attacks, 445–456.

B. den Boer, A. Bosselaers, An attack on the last two rounds of MD4, 194-203.

Y. Desmedt, Y. Frankel, Shared generation of authenticators and signatures, 457469.

C. Dwork, On verification in secret sharing, 114-128.

M.J. Fischer, R.N. Wright, Multiparty secret key exchange using a random deal of cards, 141-155.

K.R. Iversen, A cryptographic scheme for computerized general elections, 405-419.

J. Kilian, R. Rubinfeld, Interactive proofs with space bounded provers, 225-231.

N. Koblitz, CM-Curves with good cryptographic properties, 279-287.

K. Koyama, U.M. Maurer, T. Okamoto, S.A. Vanstone, New public-key schemes based on elliptic curves over the ring Z_n , 252-266.

D. Lapidot, A. Shamir, A one-round, two-prover, zero-knowledge protocol for NP, 213-224.

M. Luby, Pseudo-random generators from one-way functions, 300.

S. Micali, P. Rogaway, Secure computation, 392–404.

H. Morita, K. Ohta, S. Miyaguchi, A switching closure test to analyze cryptosystems, 183-193.

T. Okamoto, K. Ohta, Universal electronic cash, 324-337.

T. Okamoto, K. Sakurai, Efficient algorithms for the construction ofhyperelliptic cryptosystems, 267-278.

J. Patarin, New results on pseudorandom permutation generators based on the DES scheme, 301-3 12.

T.P. Pedersen, Non-interactive and information-theoretic secure verifiable secret sharing, 129-140.

B. Pfitzmann, M. Waidner, How to break and repair a ‘provably secure” untraceable payment system, 338-350.

C. Rackoff, D.R. Simon, Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, 433-444.

S. Rudich, The use of interaction in public cryptosystems, 242-25 1.

D.R. Stinson, Combinatorial characterizations of authentication codes, 62-73.

D.R. Stinson, Universal hashing and authentication codes, 74-85.

A. Tardy-Corfdir, H. Gilbert, A known plaintext attack of FEAL-4 and FEAL-6, 172-182.

S.-H. Teng, Functional inversion and communication complexity, 232-241.

M.-J. Toussaint, Deriving the complete knowledge ofparticipants in cryptographic protocols, 24-43.

S. Tsujii, J. Chao, A new ID-based key sharing system, 288-299.

C.D. Walter, Faster modular multiplication by operand scaling, 313-323.

Advances in Cryptology – CRYPTO ‘92. Springer-Verlag LNCS 740 (1993).
Editor: E.F. Brickell.

T. Baritaud, M. Campana, P. Chauvaud, H. Gilbert, On the security of the permuted kernel identification scheme, 305-3 11.

A. Beimel, B. Chor, Universally ideal secret sharing schemes, 183-195.

M. Bellare, 0. Goldreich, On defining proofs of knowledge, 390-420.

M. Bellare, M. Yung, Certifying cryptographic tools: The case of trapdoor permutations, 442-460.

E. Biham, A. Shamir, Differential cryptanalysis of the full 16-round DES, 487496.

B. Blakley, G.R. Blakley, A.H. Chan, J.L. Massey, Threshold schemes with disenrollment, 540–548.

C. Blundo, A. De Santis, L. Gargano, U. Vaccaro, On the information rate ofsecretsharingschemes, 148-167.

C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, Perfectly-secure key distribution for dynamic conferences, 471-486.

Advances in Cryptology – CRYPTO '94. Springer-Verlag LNCS 839 (1994).
Editor: Y.G. Desmedt.

M. Bellare, O. Goldreich, S. Goldwasser, Incremental cryptography: The case of hashing and signing, 216–233.

M. Bellare, J. Kilian, P. Rogaway, The security of cipher block chaining, 341-358.

T. Beth, D.E. Lazic, A. Mathias, Cryptanalysis of cryptosystems based on remote chaos replication, 3 18–331.

I. Biehl, J. Buchmann, C. Thiel, Cryptographic protocols based on discrete *logarithms* in real-quadratic orders 56–60.

J. Bierbrauer, K. Gopalakrishnan, D.R. Stinson, Bounds for resilient functions and orthogonal arrays, 247–256.

D. Bleichenbacher, U.M. Maurer, Directed acyclic graphs, one-way functions and digital signatures, 75–82.

C. Blundo, A. De Santis, G. Di Crescenzo, A.G. Gaggia, U. Vaccaro, Multi-secret sharing schemes, 150–163.

M. Burmester, On the risk of opening distributed keys, 308–317.

R. Canetti, A. Herzberg, Maintaining security in the presence of transient faults, 425-438.

J. Chao, K. Tanada, S. Tsujii, Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks, 50-55.

B. Chor, A. Fiat, M. Naor, Tracing traitors, 257-270.

D. Coppersmith, Attack on the cryptographic scheme *NIKS-TAS,* 294-307.

R. Cramer, I. Damgård, B. Schoenmakers, Proofs of partial knowledge and simplified design of witness hiding protocols, 174-187.

D. Davis, R. Ihalca, P. Fenstermacher, Cryptographic randomness from air turbulence in disk drives, 114–120.

0. Delos, J.-J. Quisquater, An identity-based signature scheme with bounded life-span, 83-94.

C. Dwork, M. Naor, An efficient existentially *unforgeable* signature scheme *and its* applications, 234-246.

C. Gehrmann, *Cryptanalysis* of the *Gemmell* and Naor multiround authentication protocol, 121-128.

H. Gilbert, P. Chauvaud, A chosen plaintext attack of the *16-round* Khufu cryptosystem, 359-368.

M. Girault, J. Stem, On the length of cryptographic hash-values used in identification schemes, 202-215.

T. Horváth, S.S. Magliveras, T. van Trung, A *parallel permutation* multiplier for a PGM Crypto-chip, 108–113.

T. Itoh, Y. Ohta, H. Shizuya, Language dependent secure bit commitment, 188-201.

B.S. Kaliski Jr., M.J.B. Robshaw, Linear *cryptanalysis* using multiple approximations, 26-39.

H. Krawczyk, LFSR-based hashing and authentication, 129-139.

K. Kurosawa, New bound on authentication code with arbitration, 140-149.

E. Kushilevitz, A. Rosén, A randomness-rounds tradeoffin private computation, 397410.

S.K. Langford, M.E. Hellman, Differential-linear *cryptanalysis,* 17-25.

C.H. Lim, P.J. Lee, More *flexible* exponentiation with *precomputation,* 95-107.

J.L. Massey, S. Serconek, A Fourier transform approach to the linear complexity of nonlinearly filtered sequences, 332-340.

M. Matsui, The first experimental cryptanalysis of the Data Encryption Standard, l-l 1.

U.M. Maurer, Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms, 271-281.

I? Mihailescu, Fast generation of provable primes using search in arithmetic progressions, 282-293.

K. Ohta, K. Aoki, Linear *cryptanalysis* of the Fast Data Encipherment Algorithm, 12-16.

T. Okamoto, Designated confirmer signatures and public-key encryption are equivalent, 61-74.

K. Sako, J. Kilian, Secure voting using partially compatible homomorphisms, 411424.

J. Sebeny, X.-M. Zhang, Y. Zheng, Pitfalls in designing substitution boxes, 383-396.

J. Stem, Designing identification schemes with keys of short size, 164-173.

J.-F'. Tillich, G. Zémor, Hashing with SL_2, 40-49.

Y. Tsunoo, E. Okamoto, T. Uyematsu, *Ciphertext* only attack for one-way function of the MAP using one ciphertext, 369-382.

Advances in Cryptology – CRYPTO '93. Springer-Verlag LNCS 773 (1994).
Editor: D.R. Stinson.

L.M. Adleman, J. Demarrais, A subexponential algorithm for discrete logarithms over all finite fields, 147-158.

Y. Aumann, U. Feige, One message proof systems with known space verifiers, 85-99.

A. Beimel, B. Chor, Interaction in key distribution schemes, 444–455.

M. Bellare, P. Rogaway, Entity authentication and key distribution, 232-249.

I. Ben-Aroya, E. Biham, Differential cyptanalysis of Lucifer, 187-199.

J. Bierbrauer, T. Johansson, G. Kabatianskii, B. Smeets, On families *of hash* functions viageometric codes and concatenation, 331-342.

A. Blum, M. Furst, M. Keams, R.J. Lipton, Cryptographic primitives based on hard learning problems, 278-29 1.

C. Blundo, A. Cresti, A. De Santis, U. Vaccaro, Fully dynamic secret sharing schemes, 110–125.

A. Bosselaers, R. Govaerts, J. Vandewalle, Comparison of three modular reduction functions, 175-186.

S. Brands, Untraceable off-line cash in wallets with observers, 302-318.

J. Buchmann, J. Loho, J. Zayer, An implementation of the general number field sieve, 159-165.

D. Coppersmith, H. Krawczyk, Y. Mansour, The shrinking generator, 22-39.

D. Coppersmith, J. Stem, S. Vaudenay, Attacks on the *birational permutation* signature schemes, 435–443.

C. Crépeau, J. Kilian, Discreet solitary games, 3 19-330.

J. Daemen, R. Govaerts, J. Vandewalle, Weak keys for IDEA, 224-231.

I.B. Damgård, Interactive hashing can simplify zero-knowledge protocol design without computational assumptions, 100-109.

I.B. Damgård, T.P. Pedersen, B. Pfitzmann, On the existence of statistically hiding bit commitment schemes and fail-stop signatures, 250–265.

A. De Santis, G. Di Crescenzo, G. Persiano, Secret sharing and perfect zero knowledge, 73-84.

T. Denny, B. Dodson, A.K. Lenstra, M.S. Manasse, On the factorization of RSA-120, 166-174.

N. Ferguson, Extensions of single-term coins, 292-301.

A. Fiat, M. Naor, Broadcast encryption, 480–491.

M. Franklin, S. Haber, Joint encryption and message-efficient secure computation, 266-277.

P. Gemmell, M. Naor, Codes for interactive authentication, 355-367.

W. Hohl, X. Lai, T. Meier, C. Waldvogel, Security of iterated hash functions based on block ciphers, 379-390.

T. Itoh, M. Hoshi, S. Tsujii, A low communication competitive interactive proof system for promised quadratic residuosity, 61-72.

W.-A. Jackson, K.M. Martin, C.M. O'Keefe, Multisecret threshold schemes, 126-135.

T. Johansson, On the construction of perfect authentication codes that permit arbitration, 343-354.

H. Krawczyk, Secret sharing made short, 136-146.

T. Leighton, S. Micali, Secret-key agreement without public-key cryptography, 456-479.

C.-M. Li, T. Hwang, N.-Y. Lee, Remark on the threshold RSA signature scheme, 413419.

C.H. Lim, P.J. Lee, Another method for attaining security against adaptively chosen ciphertext attacks, 420–434.

L. O'Connor, On the distribution of characteristics in composite permutations, 403412.

K. Ohta, M. Matsui, Differential attack on message authentication codes, 200-211.

J. Patarin, P. Chauvaud, Improved algorithms for the permuted kernel problem, 391402.

B. Preneel, R. Govaerts, J. Vandewalle, Hash functions based on block ciphers: A synthetic approach, 368-378.

B. Preneel, M. Nuttin, V. Rijmen, J. Buelens, Cryptanalysis of the *CFB* mode of the DES with a reduced number of rounds, 212-223.

J. Sebeny, X.-M. Zhang, Y. Zheng, Nonlinearly balanced Boolean functions and their propagation characteristics, 49-60.

A. Shamir, Efficient signature schemes based on birational permutations, 1-12.

J. Stem, A new identification scheme based on syndrome decoding, 13-21.

R. Taylor, An integrity check value algorithm for stream ciphers, 40–48.

Advances in Cryptology – **CRYPTO** '96. Springer-Verlag LNCS 1109 (1996).
Editor: N. Koblitz.

M. Atici, D. Stinson, Universal hashing and multiple authentication, 16–30.

M. Bellare, R. Canetti, H. Krawczyk, Keying hash functions for message authenticaion, 1-15.

C. Blundo, L. Mattos, D. Stinson, Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution, 388-401.

D. Boneh, R. Lipton, Algorithms for black-box fields and their application to cryptography, 283-297.

D. Boneh, R. Venkatesan, Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes, 129-142.

A. Bosselaers, R. Govaerts, J. Vandewalle, Fast hashing on the Pentium, 298-312.

P. Camion, A. Canteaut, Generalization of *Siegenthaler* inequality and *Schnorr–Vaudenay multipermutations*, 373-387.

R. Cramer, I. Damgård, New generation of secure and practical RSA-based signatures, 173-185.

S. Droste, New results on visual cryptography, 402–416.

R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, Robust and efficient sharing of RSA functions, 157-172.

S. Halevi, S. Micali, Practical and provably-secure commitment schemes from collision-free hashing, 201-215.

T. Helleseth, T. Johansson, Universal hash functions from exponential sums over finite fields and Galois rings, 3 l-44.

R. Hughes, G. Luther, G. Morgan, C. Peterson, C. Simmons, Quantum cryptography over underground optical fibers, 329-343.

M. Jakobsson, M. Yung, Proving without knowing: On oblivious, agnostic and blindfolded provers, 186-200.

J. Kelsey, B. Schneier, D. Wagner, Key-schedule cryptanalysis of IDEA, G-DES, COST, SAFER, and Triple-DES, 237-25 1.

J. Kilian, P. Rogaway, How to protect DES against exhaustive key search, 252-267.

L. Knudsen, W. Meier, Improved differential attacks on RC5, 216-228.

P. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, 104-l 13.

S. Langford, Weaknesses in some threshold cryptosystems, 74-82.

J. Massey, S. Serconek, Linear complexity of periodic sequences: A general theory, 359-372.

U. Maurer, S. Wolf, Diffie-Hellman oracles, 268-282.

D. Mayers, Quantum key distribution and string oblivious transfer in noisy channels, 344–358.

M. Nlslund, All bits in ax + b mod p are hard, 114-128.

J. Patarin, Asymmetric cryptography with a hidden monomial, 45-60.

C. Schnorr, Security of 2^t*-root* identification and signatures, 143-156.

V. Shoup, On fast and provably secure message authentication based on universal hashing, 313-328.

D. Simon, Anonymous communication and anonymous cash, 61-73.

P. van Oorschot, M. Wiener, Improvingimplementable meet-in-the-middle attacks by orders ofmagnitude, 229-236.

S. Vaudenay, Hidden collisions on DSS, 83-88.

A. Young, M. Yung, The dark side of 'black-box' cryptography, or: Why should we trust Capstone?, 89-103.

Prev. Chapter Prev. Page Home Next Page

Advances in Cryptology – **CRYPTO** '95. Springer-Verlag LNCS 963 (1995).
Editor: D. Coppersmith.

R. Anderson, R. Needham, Robustness principles for public key protocols, 236-247.

D. Beaver, Precomputing oblivous transfer, 97–109.

P. Béguin, J.-J. Quisquater, Fast server-aided RSA signatures secure against active attacks, 57-69.

A. Beimel, B. Chor, Secret sharing with public reconstruction, 353-366.

M. Bellare, R. Guérin, P. Rogaway, XOR MACs: New methods for message authentication using finite pseudorandom functions, 15-28.

G.R. Blakley, G.A. Kabatianskii, On general perfect secret sharing schemes, 367-371.

D. Bleichenbacher, W. Bosma, A.K. Lenstra, Some remarks on Lucas-based cryptosystems, 386-396.

D. Boneh, R.J. Lipton, Quantum cryptanalysis of hidden linear functions, 424–437.

D. Boneh, J. Shaw, Collusion-secure fingerprinting for digital data, 452-465.

R. Cramer, I. Damgård, Secure signature schemes based on interactive protocols, 297-310.

C. Crépeau, J. van de Graaf, A. Tapp, Committed oblivious transfer and private multi-party computation, 110-123.

I. Damgård, 0. Goldreich, T. Okamoto, A. Wigderson, Honest verifier vs. dishonest verifier in public coin zero-knowledge proofs, 325-338.

B. Dodson, A.K. Lenstra, NFS with four large primes: An explosive experiment, 372-385.

Y. Frankel, M. Yung, Cryptanalysis of the immunized LL public key systems, 287-296.

Y. Frankel, M. Yung, Escrow encryption systems visited: Attacks, analysis and designs, 222-235.

S. Halevi, Efficient commitment schemes with bounded sender and unbounded receiver, 84-96.

A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, Proactive secret sharing or: How to cope with perpetual leakage, 339-352.

B.S. Kaliski Jr., Y.L. Yin, On differential and linear cryptanalysis of the RC5 encryption algorithm, 171-184.

J. Kilian, Improved efficient arguments, 311-324.

J. Kilian, T. Leighton, Fair cryptosystems, revisited: A rigorous approach to key-escrow, 208–221.

A. Klapper, M. Goresky, Cryptanalysis based on 2-adic rational approximation, 262-273.

L.R. Knudsen, A key-schedule weakness in SAFER K-64, 274-286.

K. Kurosawa, S. Obana, W. Ogata, t-cheater identifiable (k, n) threshold secret sharing schemes, 410-423.

S.K. Langford, Threshold DSS signatures without a trusted party, 397–409.

A.K. Lenstra, P. Winkler, Y. Yacobi, A key escrow system with warrant bounds, 197-207.

C.H. Lim, P.J. Lee, Security and performance of server-aided RSA computation protocols, 70-83.

D. Mayers, On the security of the quantum oblivious transfer and key distribution protocols, 124-135.

S. Micali, R. Sidney, A simple method forgenerating and sharing pseudo-random functions, with applications to Clipper-like key escrow systems, 185-196.

K. Ohta, S. Moriai, K. Aoki, Improving the search algorithm for the best linear expression, 157-170.

T. Okamoto, An efficient divisible electronic cash scheme, 438-451.

S.-J. Park, S.-J. Lee, S.-C. Goh, On the security of the Gollmann cascades, 148-156.

J. Patarin, Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88, 248-261.

B. Preneel, P. van Oorschot, MDx-MAC and building fast MACs from hash functions, 1-14.

P. Rogaway, Bucket hashing and its application to fast message authentication, 29–42.

R. Schroeppel, H. Orman, S. O'Malley, 0. Spatscheck, Fast key exchange with elliptic curve systems, 43-56.

T. Theobald, How to break Shamir's asymmetric basis, 136-147.

M. Davio, Y. Desmedt, J.-J. Quisquater, Propogation characteristics of the DES, 62-73.

J.A. Davis, D.B. Holdridge, G.J. Simmons, Status report on factoring (at the *Sandia* National Labs), 183-215.

P. Delsarte, Y. Desmedt, A. Odlyzko, P. Piret, Fast *cryptanalysis* of the *Matsumoto-Imai* public key scheme, 142-149.

A, Ecker, Time-division multiplexing scramblers: Selecting permutations and testing the systems, 399-415.

Y. Girardot, Bull *CP8* smart card uses in cryptology, 464–469.

0. Goldreich, On concurrent identification protocols, 387-396.

0. Goldreich, On the number of close-and-equal pairs of bits in a string (with implications on the security *of RSA's L.S.B),* 127-141.

D. Gollmann, Pseudo random properties of cascade connections of clock controlled shift registers, 93-98.

R.M.F. Goodman, A.J. McAuley, A new trapdoor knapsack public-key cryptosystem, 150-158.

J. Gordon, Strong primes are easy to find, 216-223.

J. Goutay, Smart card applications in security and data protection, 459-463.

H. Groscot, Estimation of some encryption functions implemented into smart cards, 470-479.

L.C. Guillou, Smart cards and conditional access, 480-489.

S. Harari, Non-linear, non-commutative functions for data integrity, 25-32.

R.W. Jones, User functions for the generation and distribution of encipherment keys, 3 17-334.

R. Lidl, On cryptosystems based on polynomials and finite fields, 10-15.

J.L. Massey, R.A. Rueppel, Linear ciphers and random sequence generators with multiple clocks, 74-87.

A.M. Odlyzko, Discrete logarithms in finite fields and their cryptographic significance, 224-314.

L.H. Ozarow, A.D. Wyner, Wire-tap channel II, 33-50.

J.P. Pieprzyk, Algebraical structures of cryptographic transformations, 16-24.

C. Pomerance, The quadratic sieve factoring algorithm, 169-182.

R. Rivest, RSA chips (past/present/future), 159-165.

G. Ruggiu, Cryptology and complexity theories, 3-9.

I. Schaumueller-Bichl, E. Piller, A method of software protection based on the use of smart cards and cryptographic techniques, 446–454.

C.P. Schnorr, W. Alexi, RSA-bits are 0.5 + ϵ secure, 113-126.

S.C. Serpell, C.B. Brookson, Encryption and key management for the ECS satellite service, 426-436.

A. Sgarro, Equivocations for homophonic ciphers, 51-61.

G.J. Simmons, The subliminal channel and digital signatures, 364-378.

B.J.M. Smeets, On the use of the binary multiplying channel in a private communication system, 339-348.

A. Turbat, Session on smart cards -introductory remarks, 457–458.

R. Vogel, On the linear complexity of cascaded sequences, 99-109.

Advances in Cryptology – **EUROCRYPT** '85, Linz, Austria. Springer-Verlag LNCS 219 (1986).
Editor: F. Pichler.

G.B. Agnew, Modelingofencryption techniques forsecrecyandprivacyin multi-usernetworks, 221-230.

J. Bemasconi, C.G. Gilnther, Analysis of a nonlinear feedforward logic for binary sequence generators, 161-166.

R.V. Book, F. Otto, The verifiability of two-party protocols, 254-260.

R.L. Bradey, I.G. Graham, Full encryption in a personal computer system, 23 l-240.

L. Brynielsson, On the linear complexity of combined shift register sequences, 156-160.

D. Chaum, Showing credentials without identification signatures transferred between unconditionally *unlinkable* pseudonyms, 241-244.

D.-S. Chen, Z.-D. Dai, On feedforward transforms and p-fold periodic p-arrays, 130–134.

D.W. Davies, W.L. Price, Engineering secure information systems, 191-199.

P. Godlewski, G.D. Cohen, Authorized writing for "write-once" memories, 111-115.

T. Herlestam, On functions of linear shift register sequences, 119–129.

O.J. Horak, The contribution of E.B. Fleissner and A. *Figl* for today's cryptography, 3-17.

R.W. Jones, M.S.J. Baxter, The role of encipherment services in distributed systems, 214-220.

A.3 Eurocrypt Proceedings

Cryptography – Proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, 1982.
Springer-Verlag LNCS 149 (1983).
Editor: T. Beth.

No Author, Introduction, l-28.
No Author, Mechanical cryptographic devices, 47–48.
EL. Bauer, Cryptology-methods and maxims, 31-46.
H.J. Beker, *Analogue* speech security systems, 130-146.
D.W. Davies, G.I.P. Parkin, The average cycle size of the key stream in output feedback encipherment, 263-279.
M. Davio, J.-M. Goethals, J.-J. Quisquater, Authentication procedures, 283-288.
A. Ecker, Finite semigroups and the RSA-cryptosystem, 353-369.
R. Eier, H. Lagger, Trapdoors in knapsack cryptosystems, 316-322.
J.A. Gordon, H. Retkin, Are big S-boxes best?, 257-262.
L. Győrfi, I. Kerekes, Analysis of multiple access channel using multiple level FSK, 165-172.
T. Herlestam, On using prime polynomials in *crypto* generators, 207-216.
P. Hess, K. Wirl, A voice scrambling system for testing and demonstration, 147-156.
L. Horbach, Privacy and data protection in medicine, 228-232.
I. Ingemarsson, A new algorithm for the solution of the knapsack problem, 309-3 15.
S.M. Jennings, Multiplexed sequences: Some properties of the minimum polynomial, 189-206.
A.G. Konheim, Cryptanalysis of a *Kryha* machine, 49-64.
M. Mignotte, How to share a secret, 371-375.
M.R. Oberman, Communication security in remote controlled computer systems, 219-227.
F. Pichler, Analog scrambling by the general fast Fourier transform, 173-178.
EC. Piper, Stream ciphers, 181-188.
J. Sattler, C.P. Schnorr, Ein effizienzvergleich der faktorisierungsverfahren von Morrison-Brillhart und Schroeppel, 33 l-35 1.
I. Schaumiiller-Bichl, Cryptanalysis of the Data Encryption Standard by the method offonnal coding, 235-255.
C.P. Schnorr, *Is* the RSA-scheme safe?, 325-329.
P. Schöbi, J.L. Massey, Fast authentication in a trapdoor-knapsack public key cryptosystem, 289-306.
H.-R. Schuchmann, Enigma variations, 65-68.
N.J.A. Sloane, Encrypting by random rotations, 71-128.
K.-P Timmann, The rating of understanding in secure voice communications systems, 157-163.

Advances in Cryptology – Proceedings of **EUROCRYPT 84,** Paris, France.
Springer-Verlag LNCS 209 (1985).
Editors: T. Beth, N. Cot, and I. Ingemarsson.

G.B. Agnew, Secrecy and privacy in a local area network environment, 349-363.
R. Berger, R. Peralta, T. Tedrick, A provably secure oblivious transferprotocol, 379-386.
T. Beth, EC. Piper, The stop-and-go generator, 88-92.
R. Blom, An optimal class of symmetric key generation systems, 335-338.
A. Bouckaert, Security of transportable computerized files, 416-425.
0. Brugia, S. Improta, W. Wolfowicz, An encryption and *authentification* procedure for tele-surveillance systems, 437-445.

W.B. Miiller, R. Nöbauer, On commutative semigroups of polynomials and their applications in cryptography.

Q.A. Nguyen, Elementary proof of Rueppel's linear complexity conjecture.

R. Peralta, A simple and fast probabilistic algorithm for computing square roots modulo a prime number.

F. Pichler, On the Walsh-Fourier analysis of correlation-immune switching functions.

D. Pinkas, B. Transac, The need for a standardized compression algorithm for digital signatures.

W.L. Price, The NPL intelligent token and its application.

R.A. Rueppel, O.J. Staffelbach, Products of linear recurring sequence with maximum complexity.

P. Schöbi, Perfect authentication systems for data sources with arbitrary statistics.

T. Siegenthaler, Correlation-immune polynomials over finite fields.

B. Smeets, Some properties of sequences generated by a windmill machine.

M.Z. Wang, J.L. Massey, The characterization of all binary sequences with perfect linear complexity *profiles.*

Advances in Cryptology – **EUROCRYPT '87,** Amsterdam, The Netherlands.
Springer-Verlag LNCS 304 (1988).
Editors: D. Chaum and W.L. Price.

G.B. Agnew, Random sources for cryptographic systems, 77-81.

D.P. Anderson, P.V. Rangan, High-performance interface architectures for cryptographic hardware, 301–309.

H.J. Beker, G.M. Cole, Message authentication and dynamic passwords, 171-175.

A. Beutelspacher, Perfect and essentially perfect authentication schemes, 167-170.

E.F. Brickell, Y. Yacobi, On privacy homomorphisms, 117-125.

D. Chaum, Blinding for unanticipated signatures, 227-233.

D. Chaum, J.-H. Evertse, J. van de Graaf, An improved protocol for demonstrating possession of discrete logarithms and some generalizations, 127-141.

A.J. Clark, Physical protection of cryptographic devices, 83-93.

I.B. Damgård, Collision free hash functions and public key signature schemes, 203-216.

G.I. Davida, G.G. Walter, A public key analog cryptosystem, 143-147.

J.-H. Evertse, Linear structures in blockciphers, 249-266.

M. Girault, Hash-functions using modulo-n operations, 217-226.

C.G. Günther, Alternating step generators controlled by de Bruijn sequences, 5-14.

C.J.A. Jansen, D.E. Boekee, Modes of blockcipher algorithms and their protection against active eavesdropping, 28 l-286.

F. Jorissen, J. Vandewalle, R. Govaerts, Extension of Brickell's algorithm for breaking high density knapsacks, 109–115.

J.L. Massey, U. Maurer, M. Wang, Non-expanding, key-minimal, robustly-perfect, linear and bilinear ciphers, 237-247.

S. Mund, D. Gollmann, T. Beth, Some remarks on the cross correlation analysis of pseudo random generators, 25-35.

H. Niederreiter, Sequences with almost perfect linear complexity profile, 37-5 1.

F. Pichler, Finite state machine modelling of cryptographic systems in loops, 65-73.

R.A. Rueppel, When shift registers clock themselves, 53-64.

I. Schaumiiller-Bichl, IC-Cards in high-security applications, 177-199.

H. Sedlak, The RSA cryptography processor, 95-105.

A. Shitnizu, S. Miyaguchi, Fast data encipherment algorithm FEAL, 267-278.

T. Siegenthaler, A.W. Kleiner, R. Forré, Generation of binary sequences with controllable complexity and ideal r-tupel distribution, 15-23.

G.J. Simmons, Message authentication with arbitration of transmitter/receiver disputes, 15 l-l 65.

I. Verbauwhede, F. Hoomaert, J. Vandewalle, H. De Man, Security considerations in the design *and implementation* of a new DES chip, 287-300.

B.S. Kaliski Jr., R.L. Rivest, A.T. Sherman, *Is* the Data Encryption Standard a group?, 81-95.

M. Kowatsch, B.O. Eichinger, F.J. Seifert, Message protection by spread spectrum modulation in a packet voice radio link, 273-277.

T. Krivachy, The *chipcard* -an identification card with cryptographic protection, 200-207.

M.-L. Liu, Z.-X. Wan, Generalized multiplexed sequences, 135-141.

H. Meijer, S. Akl, Two new secret key cryptosystems, 96-102.

W.B. Müller, R. Nöbauer, Cryptanalysis of the Dickson-scheme, 50-61.

H. Niederreiter, A public-key cryptosystem based on shift register sequences, 35-39.

R. Peralta, Simultaneous security of bits in the discrete log, 62-72.

A. Pfitzmann, M. Waidner, Networks without user observability – design options, 245-253.

J.P. Pieprzyk, On public-key cryptosystems built using polynomial rings, 73-78.

U. Rimensberger, Encryption: Needs, requirements and solutions in banking networks, 208-213.

R.L. Rivest, A. Shamir, Efficient factoring based on partial information, 31-34.

R. A. Rueppel, Linear complexity and random sequences, 167-l 88.

T. Siegenthaler, Cryptanalysts representation of nonlinearly filtered ML-sequences, 103-l 10.

G.J. Simmons, The practice of authentication, 261-272.

B. Smeets, A comment on Niederreiter's public key cryptosystem, 40–42.

B. Smeets, A note on sequences generated by clock controlled shift registers, 142-148.

T. Tedrick, On the history of cryptography during WW2, and possible new directions for cryptographic research, 18-28.

J. Vandewalle, R. Govaerts, W. De Becker, M. Decroos, G. Speybrouck, Implementation study of public key cryptographic protection in an existing electronic mail *and* document handling system, 43–49.

N.R. Wagner, P.S. Putter, M.R. Cain, Using algorithms as keys in stream ciphers, 149-155.

EUROCRYPT 86, Linköping, Sweden.
Abstracts of papers (no conference proceedings were published).
Program Chair: J.L. Massey.

G. Agnew, Another look at redundancy in cryptographic systems.

A. Bauval, Crypanalysis of pseudo-random number sequences generated by a linear congruential recurrence of gi ven order.

M. Beale, Properties of de Bruijn sequences generated by a cross-join technique.

A. Beutelspacher, Geometric structures as threshold schemes.

E.F. Brickell, *Cryptanalysis* of the Yagisawa public key cryptosystem.

D.D. Buckley, M. Beale, Public key encryption of stream ciphers.

H. Cloetens, Y. Desmedt, L. Bierens, J. Vandewalle, R. Govaerts, Additional properties in the S-boxes of the DES.

G.I. Davida, Y.-S. Yeh, Multilevel cryptosecure relational databases.

Y. Desmedt, F. Hoornaert, J.-J Quisquater, Several exhaustive key search machines and DES.

G. Dial, F. Pessoa, *Sharma-Mittal* entropy and Shannon's random cipher result.

A. Ecker, Tactical configurations and threshold schemes.

V. Fåk, Activities of *IFIP* working group *11:4* on *crypto* management.

0. Frank, P. Weidenman, Controlling individual information in statistics by coding.

A.S. Glass, Could the smart card be dumb?

D. Gollmann, Linear complexity of sequences with *period* p^n.

C.G. Günther, On some properties of the sum of two pseudorandom generators.

F.-P Heider, D. Kraus, M. Welschenbach, Some preliminary remarks on the decimal, shift and *add*-algorithm (DSA).

T. Herlestam, On linear shift registers with permuted feedback.

N.S. James, R. Lidl, H. Niederreiter, A cryptanalytic attack on the CADE cryptosystem.

C.J.A. Jansen, Protection against active eavesdropping.

R.A. Kemmerer, Analyzing encryption protocols using format verification techniques.

D.S.P. Khoo, G.J. Bird, J. Sebeny, Encryption exponent 3 and the security of RSA.

J.H. Moore, Cycle structure of the weak and semi-weak DES keys.

Advances in **Cryptology-EUROCRYPT** '89, Houthalen, Belgium. Springer-Verlag LNCS 434 (1990). Editors: J.-J. Quisquater and J. Vandewalle.

G.B. Agnew, R.C. Mullin, S.A. Vanstone, A fast elliptic curve cryptosystem, 706-708.

M. Antoine, J.-F Brakeland, M. Eloy, Y. Poullet, Legal requirements facing new signature technologies, 273-287.

F. Bauspieß, H.-J. Knobloch, How to keep authenticity alive in a computer network, 38-46.

M. Bettilsson, E.F. Brickell, I. Ingemarsson, Cryptanalysis of video encryption based on space-filling curves, 403-411.

T. Beth, Z.-D. Dai, On the complexity of pseudo-random sequences -or: If you can describe a sequence it can't be random, 533-543.

A. Beutelspacher, How to say "no", 491-496.

J. Bos, B. den Boer, Detection of disrupters in the *DC protocol,* 320-327.

W. Bosma, M.-P van der Hulst, Fasterprimality testing, 652-656.

J. Boyar, K. Friedl, C. Lund, Practical zero-knowledge proofs: Giving hints and using deficiencies, 155–172.

C. Boyd, A new multiple key cipher and an improved voting scheme, 617-625.

G. Btassard, How to improve signature schemes, 16-22.

G. Brassard, C. Crepeau, Sorting out zero-knowledge, 181-191.

G. Brassard, C. Crepeau, M. Yung, Everything in NP can be *argued* in perfect zero-knowledge in a bounded number of rounds, 192–195.

E.F. Brickell, Some ideal secret sharing schemes, 468–475.

L. Brown, J. Seberry, On the design of permutation P in DES type cryptosystems, 696-705.

J.A. Buchmann, S. Düllmann, H.C. Williams, On the complexity and efficiency of a new key exchange system, 597-616.

M.V.D. Bum-tester, Y. Desmedt, F. Piper, M. Walker, A general zero-knowledge scheme, 122-133.

G. Carter, Some conditions on the linear complexity profiles of certain binary sequences, 691-695.

A.H. Chan, M. Goresky, A. Klapper, On the linear complexity of feedback registers, 563-570.

D. Chaum, Online cash checks, 288-293.

D. Chaum, B. den Boer, E. van Heyst, S. Mjølsnes, A. Steenbeek, Efficient offline electronic checks, 294-301.

H. Cnudde, *CRYPTEL* – the practical protection of an existing electronic mail system, 237-242.

C. Crepeau, Verifiable disclosure of secrets and applications, 150-154.

Z.-D. Dai, K.C. Zeng, Feedforward functions defined by de Bruijn sequences, 544–548.

G. Davida, Y. Desmedt, R. Peralta, A key distribution system based on any one-way function, 75-79.

M. De Soete, K. Vedder, M. Walker, Cartesian authentication schemes, 476–490.

B. den Boer, More efficient match-making and satisfiability. The five card trick, 208-217.

W. Diffie, The adolescence of public-key cryptography, 2.

J. Domingo i Ferrer, L. Huguet i Rotger, Full secure key exchange and authentication with no previously shared secrets, 665-669.

Y. Duhoux, Deciphering bronze age scripts of Crete. The case of linear A, 649–650.

P. Flajolet, A. Odlyzko, Random mapping statistics, 329-354.

R. Forré, A fast correlation attack on nonlinearly feedforward *filtered* shift-register sequences, 586-595.

Y. Frankel, A practical protocol for large group oriented networks, 56-61.

Z. Galil, S. Haber, M. Yung, A secure public-key authentication scheme, 3-15.

P. Godlewski, C. Mitchell, Key minimal authentication systems for unconditional secrecy, 497-501.

D. Gollmann, W.G. Chambers, A cryptanalysis of step,,,-cascades, 680-687.

C.G. Giinther, An identity-based key-exchange protocol, 29-37.

C.G. Günther, Parallel generation of recurring sequences, 503-522.

T. Hwang, T.R.N. Rao, Private-key algebraic-code cryptosystems with high information rates, 657-661.

H. Isselhorst, The use of fractions in public-key cryptosystems, 47-55.

W.J. Jaburek, A generalization of El Carnal's public-key cryptosystem, 23-28.

H.N. Jendal, Y.J.B. Kuhn, J.L. Massey, An information-theoretic treatment of homophonic substitution, 382-394.

A.K. Lenstra, M.S. Manasse, Factoring by electronic mail, 355-371.

Advances in Cryptology-EUROCRYPT '88, Davos, Switzerland. Springer-Verlag LNCS 330 (1988). Editor: C. Günther.

G.B. Agnew, R.C. Mullin, S.A. Vanstone, Fast exponentiation in $GF(2^n)$, 251-255.

G.B. Agnew, R.C. Mullin, S.A. Vanstone, An interactive data exchange protocol based on discrete exponentiation, 159-166.

T. Beth, Efficient zero-knowledge identification scheme for smart cards, 77-84.

C. Boyd, Some applications of multiple key ciphers, 455–467.

J. Brandt, I.B. Damgård, P. Landrock, Anonymous and verifiable registration in databases, 167-176.

E.F. Brickell, D.R. Stinson, Authentication codes with multiple arbiters, 51-55.

W.G. Chambers, D. Gollmann, Lock-in effect in cascades of clock-controlled shift-registers, 331-343.

D. Chaum, Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA, 177-182.

G.I. Davida, Y.G. Desmedt, Passports and visas versus ID's, 183-188.

J.A. Davis, D.B. Holdridge, Factorization of large integers on a massively parallel computer, 235-243.

M. De Soete, Some constructions for authentication-secrecy codes, 57-75.

M. De Soete, K. Vedder, Some new classes ofgeometric threshold schemes, 389-401.

B. den Boer, *Cryptanalysis* of *F.E.A.L.*, 293-299.

Y. Desmedt, Subliminal-free authentication and signature, 23-33.

A. Di Porto, P. Filipponi, A probabilistic primality test based on the properties of certain generalized Lucas numbers, 21 l-223.

C. Ding, Proof of Massey's conjectured algorithm, 345-349.

M. Girault, R. Cohen, M. Campana, A generalized birthday attack, 129-156.

P. Godlewski, P. Camion, Manipulations and errors, detection and localization, 97-106.

R.N. Gorgui-Naguib, S.S. Dlay, Properties of the Euler totient function modulo 24 and some of its cryptographic implications, 267-274.

L.C. Guillou, J.-J. Quisquater, A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory, 123-128.

C.G. Günther, A universal algorithm for homophonic coding, 405–414.

F. Hoornaert, M. Decroos, J. Vandewalle, R. Govaerts, Fast RSA-hardware: Dream or reality?, 257-264.

H. Jingmin, L. Kaicheng, A new probabilistic encryption scheme, 415-418.

S. Kawamura, K. Hirano, A fast modular arithmetic algorithm using a residue table, 245-250.

S.J. Knapskog, Privacy protected payments - realization of a protocol that guarantees payer anonymity, 107–122

H.-J. Knobloch, A smart card implementation of the Fiat-Shamir identification scheme, 87-95.

K. Koyama, K. Ohta, Security of improved identity-based conference key distribution systems, 11-19.

P.J. Lee, E.F. Brickell, An observation on *the* security of McEliece's public-key cryptosystem, 275-280.

D. Lin, M. Liu, Linear recurring m-arrays, 35 l-357.

T. Matsumoto, H. Imai, Public quadratic *polynomial-tuples* for efficient signature-verification and message-encryption, 419-453.

W. Meier, 0. Staffelbach, Fast correlation attacks on stream ciphers, 301-314.

H. Niederreiter, The probabilistic theory of linear complexity, 191-209.

E. Okamoto, Substantial number of cryptographic keys *and its* application to encryption designs, 361-373.

R.A. Rueppel, Key agreements based on function composition, 3-10.

C.P. Schnorr, On the construction *of random* number generators and random function generators, 225-232.

A. Sgarro, A measure of semiequivocation, 375-387.

G.J. Simmons, G.B. Purdy, Zero-knowledge proofs of identity and veracity of transaction receipts, 35-49.

B.J.M. Smeets, W.G. Chambers, Windmill generators: A generalization and an observation of how many there are, 325-330.

S. Tezuka, A new class of nonlinear functions for running-key generators, 317-324.

B. Vallée, M. Girault, P. Toffin, How to *break Okamoto's cryptosystem by reducing lattice* bases, 281-291.

G. Davida, Y. Desmedt, R. Peralta, On the importance *of memory* resources in the security *of key* exchange protocols, 11-15.

A. De Santis, G. Persiano, Public-randomness in public-key cryptography, 46-62.

A. De Santis, M. Yung, On the design of provably secure cryptographic hash functions, 412-43 1.

B. den Boer, Oblivious transfer protecting secrecy – an implementation for oblivious transfer protecting secrecy almost unconditionally and a bitcommitment based on factoring protecting secrecy unconditionally, 3 1-45.

J. Domingo-Ferrer, Software run-time protection: A cryptographic issue, 474-480.

S.R. Dussé, B.S. Kaliski Jr., A cryptographic library for the Motorola *DSP 56000,* 230–244.

J.-H. Evertse, E. van Heyst, Which new RSA signatures can be computed from some given RSA signatures?, 83-97.

M. Girault, An identity-based identification scheme based on discrete logarithms modulo a composite number, 481-486.

J.D. Golić, M.J. Mihaljević, A noisy clock-controlled shift register cryptanalysis concept based on sequence comparison approach, 487-49 1.

L.C. Guillou, J.-J. Quisquater, M. Walker, l? Landrock, C. Shaer, Precautions taken against various potential attacks in *ISO/IEC DIS* 9796, 465-473.

T. Hwang, Cryptosystems for group oriented cryptography, 352-360.

I. Ingemarsson, G.J. Simmons, A protocol to set up shared secret schemes without the assistance of a mutually trusted party, 266-282.

C.J.A. Jansen, On the construction of run permuted sequences, 196-203.

B.S. Kaliski Jr., The MD4 message digest algorithm, 492.

K. Kurosawa, Y. Katayama, W. Ogata, S. Tsujii, General public key residue cryptosystems and mental poker protocols, 374-388.

X. Lai, J.L. Massey, A proposal for a new block encryption standard, 389404.

A.K. Lenstra, M.S. Manasse, Factoring with two large primes, 72-82.

S. Lloyd, Properties of binary functions, 124–139.

U. Maurer, A provably-secure strongly-randomized cipher, 361-373.

W. Meier, 0. Staffelbach, Correlation properties of combiners with memory in stream ciphers, 204–213.

G. Meister, On an implementation of the Mohan-Adiga algorithm, 496–500.

S. Miyaguchi, K. Ohta, M. Iwata, Confirmation that some hash functions are not collision free, 326-343.

F. Morain, Distributed primality proving and the primality of $(2^{3539}+1)/3$, 110–123.

H. Niederreiter, The linear complexity profile and the jump complexity of keystream sequences, 174-188.

V. Niemi, A new trapdoor in knapsacks, 405–411.

K. Nyberg, Constructions of bent functions and difference sets, 151-160.

K. Ohta, T. Okamoto, K. Koyama, Membership authentication for hierarchical multigroups using the extended Fiat-Shamir scheme, 446-457.

H. Ong, C.P. Schnorr, Fast signature generation with a Fiat Shamir-like scheme, 432–440.

H. Orup, E. Svendsen, E. Andreasen, VICTOR - an efficient RSA hardware implementation, 245-252.

J. Pieprzyk, How to constructpseudorandom permutations from *single pseudorandom* functions, 140-150.

B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle, Propagation characteristics of Boolean functions, 161-173.

R. Scheidler, J.A. Buchmann, H.C. Williams, Implementation of a key exchange protocol using real quadratic fields, 98-109.

A. Sgarro, Lower bounds for authentication codes with splitting, 283-293.

S. Shinozaki, T. Itoh, A. Fujioka, S. Tsujii, Provably secure key-updating schemes in identity-based systems, 16-30.

B. Smeets, P. Vanrose, Z.-X. Wan, On the construction of authentication codes with secrecy and codes withstanding spoofing attacks of order $L \geq 2$, 306-312.

J. Stem, P. Toffin, Cryptanalysis of a public-key cryptosystem based on approximations by rational numbers, 3 13-3 17.

P.C. van Oorschot, M.J. Wiener, A known-plaintext attack on two-key triple encryption, 3 18-325.

Y. Yacobi, Exponentiating faster with addition chains, 222-229.

S. Lloyd, Counting functions satisfying a *higher* order strict avalanche criterion, 63-74.

U.M. Maurer, Fast generation of secure RSA-moduli with almost maximal diversity, 636-647.

W. Meier, 0. Staffelbach, Nonlinearity criteria for cryptographic functions, 549-562.

S.F. Mjølsnes, A simple technique for diffusing cryptoperiods, 110-120.

F. Morain, *Atkin's* test: News *from* the front, 626-635.

H. Niederreiter, Keystream sequences with a good linear complexity profile for every starting point, 523-532.

T. Okamoto, K. Ohta, *Divertible* zero-knowledge interactive proofs and commutative random *self*-reducibility, 134-149.

B. Pfitzmann, A. Pfitzmann, How to break the direct RSA-implementation of *MIXes*, 373-381.

J.P. Pieprzyk, Non-linearity of exponent permutations, 80-92.

J.-J. Quisquater, A. Bouckaert, Zero-knowledge procedures for confidential access to medical records, 662-664.

J.-J. Quisquater, J.-P Delescaille, How easy is collision search? Application to DES, 429–434.

J.-J. Quisquater, M. Girault, *2n-bit* hash-functions using n-bit symmetric block cipher algorithms, 102–109.

Y. Roggeman, Varying feedback shift registers, 670–679.

R.A. Rueppel, On the security of Schnorr's pseudo random generator, 423428.

C.P. Schnorr, Efficient identification and signatures for smart cards, 688689.

A. Sgarro, Informational divergence bounds for authentication codes, 93-101.

G.J. Simmons, Prepositioned shared secret and/or shared control schemes, 436-467.

C. Siuda, Security in open distributed processing, 249-266.

J. Stem, An alternative to the Fiat-Shamir protocol, 173-l 80.

J. Van Auseloos, Technical security: The starting point, 243-248.

A. Vandemeulebroecke, E. Vanzieleghem, T. Denayer, P.G.A. Jespers, A single chip 1024 bits RSA processor, 219-236.

J. Vandewalle, D. Chaum, W. Fumy, C. Jansen, P. Landrock, G. Roelofsen, A European *call* for cryptographic Algorithms: RIPE; RACE Integrity Primitives Evaluation, 267-271.

M. Waidner, Unconditional sender and recipient untraceability in spite of active attacks, 302-3 19.

M. Waidner, B. Pfitzmann, The dining cryptographers in the disco: Unconditional sender and recipient *un*traceability with computationally secure serviceability, 690.

M. Wang, Linear complexity profiles and continued fractions, 571-585.

P. Wichmann, Cryptanalysis of a modified rotor machine, 395-402.

M.J. Wiener, Cryptanalysis of short RSA secret exponents, 372.

M. Yung, Zero-knowledge proofs of computational power, 196-207.

Y. Zheng, T. Matsumoto, H. Imai, Impossibility and optimahty results on constructingpseudorandom permutations, 412-422.

Advances in Cryptology – EUROCRYPT '90, Aarhus, Denmark. Springer-Verlag LNCS 473 (1991). Editor: I.B. Damghrd.

F. Bauspieß, H.-J. Knobloch, P. Wichmann, Inverting the pseudo exponentiation, 344-35 1.

C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, Experimental quantum cryptography, 253-265.

A. Beutelspacher, U. Rosenbaum, Essentially l-fold secure authentication systems, 294-305.

G. Bleumer, B. Pfitzmann, M. Waidner, A remark on a signature scheme where forgery can be proved, 441445.

E.F. Brickell, K.S. McCurley, An interactive identification scheme based on discrete logarithms and factoring, 63-7 1.

M.V.D. Burmester, A remark on the efficiency of identification schemes, 493–495.

M.V.D. Burmester, Y. Desmedt, All languages in *NP have divertible* zero-knowledge proofs and arguments under cryptographic assumptions, l-10.

A.H. Chan, M. Goresky, A. Klapper, Correlation functions of geometric sequences, 214-22 1.

D. Chaum, Zero-knowledge undeniable signatures, 458464.

Z.-D. Dai, T. Beth, D. Gollmann, Lower bounds for the linear complexity of sequences over residue rings, 189-195.

T.P. Pedersen, A threshold cryptosystem without a trusted party, 522-526.

J. Pieprzyk, Probabilistic analysis of elementary randomizers, 542-546.

J. Pieprzyk, R. Safavi-Naini, Randomized authentication systems, 472-481.

M. Portz, On the use of interconnection networks in cryptography, 302-315.

B. Preneel, D. Chaum, W. Fumy, C.J.A. Jansen, P. Landrock, G. Roelofsen, Race Integrity Primitives Evaluation (RIPE): A status report, 547-55 1.

B. Preneel, R. Govaerts, J. Vandewalle, Boolean functions satisfying higher order propagation criteria, 141-152.

R.A. Rueppel, A formal approach to security architectures, 387-398.

B. Sadeghiyan, J. Pieprzyk, A construction for one way hash functions and pseudorandom bit generators, 431-445.

C.P. Schnorr, Factoring integers and computing discrete logarithms via diophantine approximation, 28 1–293.

H. Shizuya, T. Itoh, K. Sakurai, On the complexity of *hyperelliptic* discrete logarithm problem, 337-35 1.

G. Zémor, Hash functions and graphs with large girths, 508-5 11.

Advances in Cryptology – EUROCRYPT ‘92, Balantonfüred, Hungary.
Springer-Verlag LNCS 658 (1993).
Editor: R.A. Rueppel.

G.B. Agnew, R.C. Mullin, S.A. Vanstone, On the development of a fast elliptic curve cryptosystem, 482-487.

P. Barbaroux, Uniform results in polynomial-time security, 297-306.

T. Baritaud, H. Gilbert, M. Girault, *FFT hashing* is not collision-free, 35–44.

D. Beaver, How to break a “secure” oblivious transfer protocol, 285-296.

D. Beaver, S. Haber, Cryptographic protocols provably secure against dynamic adversaries, 307-323.

M.J. Beller, Y. Yacobi, Batch Diffie-Hellman key agreement systems and their application to portable communications, 208-220.

T.A. Berson, Differential cryptanalysis mod 2^{32} with applications to MD5, 71-80.

I. Biehl, J. Buchmann, B. Meyer, C. Thiel, C. Thiel, Tools forproving zero knowledge, 356-365.

C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro, Graph decompositions and secret sharing schemes, 1–24.

E.F. Brickell, D.M. Gordon, K.S. McCurley, D.B. Wilson, Fast exponentiation with *precomputation,* 200-207.

D. Chaum, T.P. Pedersen, Transferred cash grows in size, 390–407.

L. Chen, I. Damgård, Security bounds for parallel versions of identification protocols, 461-466.

I. Damgård, Non-interactive circuit based proofs and non-interactive perfect zero-knowledge with preprocessing, 341-355.

B. Dixon, A.K. Lenstra, Massively parallel elliptic curve factoring, 183-193.

J.-H. Evertse, E. van Heyst, Which new RSA signatures can be computed from RSA signatures, obtained in a specific interactive protocol?, 378-389.

Y. Frankel, Y. Desmedt, Classification *of ideal* homomorphic threshold schemes over *finite abelian* groups, 25–34.

J.D. Golić, Correlation via linear sequential circuit approximation of combiners with memory, 113-l 23.

J.D. Golić, S.V. Petrović, A generalized correlation attack with a probabilistic constrained edit distance, 472476.

G. Harper, A. Menezes, S. Vanstone, Public-key cryptosystems with very small key lengths, 163-173.

R. Heiman, A note on discrete logarithms with special structure, 454-457.

R. Heiman, Secure audio teleconferencing: A practical solution, 437–448.

K. Iwamura, T. Matsumoto, H. Imai, High-speed implementation methods for RSA scheme, 221-238.

K. Iwamura, T. Matsumoto, H. Imai, Systolic arrays for modular exponentiation using Montgomery method, 477–48 1.

K. Koyama, Secure conference key distribution schemes for conspiracy attacks, 449453.

X. Lai, J.L. Massey, Hash functions based on block ciphers, 55-70.

M. Matsui, A. Yamagishi, A new method *for known* plaintext attack of FEAL cipher, 81-91.

Advances in Cryptology – **EUROCRYPT '91,** Brighton, UK. Springer-Verlag LNCS 547 (1991).
Editor: D.W. Davies.

S. Berkovits, How to broadcast a secret, 535-541.

T. Beth, F. Schaefer, Non supersingular elliptic curves for public key cryptosystems, 316-327.

E. Biham, Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT '91, 532-534.

E. Biham, A. Shamir, Differential cryptanalysis of *Feal* and N-Hash, 1-16.

C. Boyd, Enhancing secrecy by data compression: Theoretical and practical aspects, 266-280.

L. Brynielsson, The information leakage through a randomly generated function, 552-553.

M. Burmester, Y. Desmedt, Broadcast interactive proofs, 81-95.

P. Camion, J. Patarin, The knapsack hash function proposed at Crypto '89 can be broken, 39-53.

W.G. Chambers, Z.-D. Dai, On binary sequences from recursions "modulo 2" "made non-linear by the *bit*-by-bit "XOR" function, 200–204.

D. Chaum, Some weaknesses of "Weaknesses of undeniable signatures", 554-556.

D. Chaum, E. van Heyst, Group signatures, 257-265.

V. Chepyzhov, B. Smeets, On a fast correlation attack on certain stream ciphers, 176-185.

M.J. Coster, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr, An improved low-density subset sum algorithm, 54-67.

C. Crépeau, M. Sántha, On the reversibility of oblivious transfer, 106-113.

Z.-D. Dai, J.-H. Yang, Linear complexity of periodically repeated random sequences, 168-175.

M.H. Dawson, S.E. Tavares, An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks, 352-367.

P. de Rooij, On the security of the Schnorr scheme using preprocessing, 71-80.

Y. Desmedt, M. Yung, Weaknesses of undeniable signature schemes, 205-220.

A. Fujioka, T. Okamoto, S. Miyaguchi, ESIGN: An efficient digital signature implementation for smart cards, 446457.

A. Fujioka, T. Okamoto, K. Ohta, Interactive bi-proof systems and undeniable signature schemes, 243-256.

E.M. Gabidulin, A.V. Paramonov, O.V. Tretjakov, Ideals over a non-commutative ring and their application in cryptology, 482489.

J.K. Gibson, Equivalent *Goppa codes* and trapdoors to McEliece's public key *cryptosystem,* 517-521.

M. Girault, Self-certifiedpublic keys, 490–497.

B. Goldburg, E. Dawson, S. Sridharan, *The* automated cryptanalysis of analog speech scramblers, 422-430.

J.D. Golić, The number of output sequences of a binary sequence generator, 160-167.

T. Habutsu, Y. Nishio, I. Sasase, S. Mori, A secret key cryptosystem by iterating a chaotic map, 127-140.

P. Horster, H.-J. Knobloch, Discrete logarithm based protocols, 399408.

K. Huber, Some considerations concerning the selection of RSA moduli, 294-301.

C.J.A. Jansen, The maximum order complexity of sequence ensembles, 153-159.

VI. Korzhik, A.I. Turkin, Cryptanalysis of McEliece's public-key cryptosystem, 68-70.

X. Lai, J.L. Massey, S. Murphy, Markov ciphers and differential cryptanalysis, 17-38.

T. Matsumoto, H. Imai, Human identification through insecure channel, 409-421.

U.M. Maurer, New approaches to the design of self-synchronizing stream ciphers, 458–471.

U.M. Maurer, Y. Yacobi, Non-interactive public-key cryptography, 498-507.

W. Meier, 0. Staffelbach, Analysis *of pseudo* random sequences generated by cellular automata, 186-199.

M.J. Mihaljević, J.D. Golić, A comparison of cryptanalytic principles based on iterative error-correction, 527-531.

F. Morain, Building cyclic elliptic curves modulo large primes, 328-336.

W.B. Miiller, A. Oswald, Dickson pseudoprimes and primality testing, 512-516.

S. Mund, Ziv-Lempel complexity for periodic sequences and *its* cryptographic application, 114-126.

K. Nyberg, Perfect nonlinear S-boxes, 378-386.

L. O'Connor, Enumerating nondegenerate permutations, 368-377.

T. Okamoto, D. Chaum, K. Ohta, Direct zero knowledge proofs of computational power in five rounds, 96–105.

T.P. Pedersen, Distributed provers with applications to undeniable signatures, 221-242.

N. Ferguson, Single term off-line coins, 3 18-328.

R.A. Games, J.J. Rushanan, Blind synchronization of m-sequences with even span, 168-l 80.

R. Göttfert, H. Niederreiter, On the linear complexity ofproducts of shift-register sequences, 15 1-158.

G. Hornauer, W. Stephan, R. Wernsdorf, Markov ciphers and alternating groups, 453-460.

T. Johansson, G. Kabatianskii, B. Smeets, On the relation between A-codes and codes correcting independent errors, l-l 1.

K. Kurosawa, K. Okada, K. Sakano, W. Ogata, S. Tsujii, Nonperfect secret sharing schemes and *matroids,* 126-141.

M. Matsui, Linear cryptanalysis method for DES cipher, 386-397.

W. Meier, On the security of the IDEA block cipher, 371-385.

D. Naccache, Can O.S.S. be repaired? -proposal for a new practical signature scheme, 233-239.

K. Nyberg, Differentially uniform mappings for cryptography, 55-64.

L. O'Connor, On the distribution of characteristics in *bijective* mappings, 360-370.

R. Ostrovsky, R. Venkatesan, M. Yung, Interactive hashing simplifies zero-knowledge protocol design, 267-273.

C. Park, K. Itoh, K. Kurosawa, Efficient anonymous channel and all/nothing election scheme, 248-259.

C. Park, K. Kurosawa, T. Okamoto, S. Tsujii, On key distribution and authentication in mobile radio networks, 461-465.

J. Patarin, How to find and avoid collisions for the knapsack hash function, 305-3 17.

R. Safavi-Naini, L. Tombak, Optimal authentication systems, 12-27.

J. Seberry, X.-M. Zhang, Y. Zheng, On constructions and nonlinearity of correlation immune functions, 181-199.

E.S. Selmer, From the memoirs of a Norwegian cryptologist, 142-150.

G.J. Simmons, The consequences of trust in shared secret schemes, 448-452.

G.J. Simmons, Subliminal communication is easy using the DSA, 218-232.

P.C. van Oorschot, An alternate explanation of two BAN-logic "failures", 443-447.

Advances in Cryptology – **EUROCRYPT** '94, Perugia, Italy. Springer-Verlag LNCS 950 (1995).
Editor: A. De Santis

M. Bellare, P. Rogaway, Optimal asymmetric encryption, 92-l 11.

E. Biham, On *Matsui's* linear cryptanalysis, 341-355.

E. Biham, A. Biryukov, An improvement of Davies' attack on DES, 461467.

C. Blundo, A. Cresti, Space requirements for broadcast encryption, 287-298.

C. Blundo, A. Giorgio Gaggia, D.R. Stinson, On the dealer's randomness required in secret sharing schemes, 35–46.

M. Burmester, Y. Desmedt, A ***secure*** and efficient conference key distribution system, 275-286.

C. Cachin, U.M. Maurer, Linking information reconciliation and privacy amplification, 266-274.

J.L. Camenisch, J.-M. Piveteau, M.A. Stadler, Blind signatures based on the discrete logarithm problem, 428–432.

F. Chabaud, On the security of some cryptosystems based on error-correcting codes, 131-139.

F. Chabaud, S. Vaudenay, Links between differential and linear cryptanalysis, 356-365.

C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naini, Y. Zheng, Comments on Soviet encryption algorithm, 433438.

D. Chaum, Designated *confirmer* signatures, 86-91.

L. Chen, I.B. Damgård, T.P. Pedersen, Parallel divertibility of proofs of knowledge, 140-155.

L. Chen, T.P. Pedersen, New group signature schemes, 171-181.

L. Csirmaz, The size of a share must be large, 13-22.

S. D' Amiano, G. Di Crescenzo, Methodology for digital money based on general cryptographic tools, 156–170.

F. Damm, F.-P. Heider, G. Wambach, *MIMD-factorisation* on hypercubes, 400-409.

P. de Rooij, Efficient *exponentiation* using *precomputation* and vector addition chains, 389-399.

T. Eng, T. Okamoto, Single-term divisible electronic coins, 306-3 19.

M. Franklin, M. Yung, The blinding of weak signatures, 67-76.

U.M. Maurer, Factoring with an oracle, 429-436.

U.M. Maurer, A simplified *and* generalized treatment of Luby-Rackoff pseudorandom permutation generators, 239-255.

U.M. Maurer, Y. Yacobi, A remark on a non-interactive public-key distribution system, 458–460.

M. Mihaljević, J.D. Golić, Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence, 124-137.

D. Naccache, A Montgomery-suitable Fiat-Shamir-like authentication scheme, 488–491.

H. Niederreiter, C.P. Schnorr, Local randomness in candidate one-way functions, 408-419.

K. Nyberg, On the construction of highly nonlinear permutations, 92-98.

L. O'Connor, T. Snider, Suffix trees and string complexity, 138-152.

K. Ohta, T. Okamoto, A. Fujioka, Secure bit commitment function against divertibility, 324-340.

T. Okamoto, K. Sakurai, H. Shizuya, How intractable is the discrete logarithm for a general finite group, 420–428.

J. Patarin, How to construct pseudorandom and super pseudorandom permutations from one single *pseudorandom* function, 256-266.

B. Pfitzmann, M. Waidner, Attacks on protocols for server-aided RSA computation, 153-162.

R. Rueppel, A. Lenstra, M. Smid, K. McCurley, Y. Desmedt, A. Odlyzko, P. Landrock, The Eurocrypt '92 controversial issue: trapdoor primes and moduli, 194–199.

B. Sadeghiyan, J. Pieprzyk, A construction forsuperpseudorandom permutations from a *single pseudorandom* function, 267-284.

J. Sauerbrey, A. Dietel, Resource requirements for the application of addition chains in modulo *exponentiation*, 174-182.

C.P. Schnorr, *FFT-Hash II*, efficient cryptographic hashing, 45-54.

A. Sgarro, Information-theoretic bounds for authentication frauds, 467471.

E. van Heyst, T.P. Pedersen, How to *make* efficient fail-stop signatures, 366-377.

R. Wemsdorf, The one-round functions of the DES generate the alternating group, 99-l 12.

Advances in Cryptology – EUROCRYPT '93, Lofthus, Norway. Springer-Verlag LNCS 765 (1994). Editor: T. Helleseth.

D. Beaver, N. So, Global, unpredictable bit generation without broadcast, 424-434.

J. Benaloh, M. de Mare, One-way accumulators: A decentralized alternative to digital signatures, 274–285.

T. Beth, C. Ding, On almost perfect nonlinear permutations, 65-76.

E. Biham, New types of cryptanalytic attacks using related keys, 398-409.

S. Blackbum, S. Murphy, J. Stem, Weaknesses of a public-key cryptosystem based on *factorizations* of finite groups, 50-54.

C. Boyd, W. Mao, On a limitation of BAN logic, 240-247.

S. Brands, D. Chaum, Distance-boundingprotocols, 344-359.

G. Brassard, L. Salvail, Secret key reconciliation by public discussion, 410-423.

M. Burrnester, Cryptanalysis of the Chang-Wu-Chen key distribution system, 440-442.

C. Carlet, Two new classes of bent functions, 77–101.

M. Carpentieri, A. De Santis, U. Vaccaro, Size of shares and probability of cheating in threshold schemes, 118-125.

R.J.F. Cramer, T.P. Pedersen, Improved privacy in wallets with observers, 329-343.

T.W. Cusick, Boolean functions satisfying a higher order strict avalanche criterion, 102-117.

J. Daemen, R. Govaerts, J. Vandewalle, Resynchronization weaknesses in synchronous stream ciphers, 159-167.

I.B. Damgård, Practical and provably secure release of a secret and exchange of signatures, 200-217.

I.B. Damglrd, L.R. Knudsen, The breaking of the AR hash function, 286-292.

P. de Rooij, On Schnorr's preprocessing for digital signature schemes, 435–439.

N. Demytko, A new elliptic curve based analogue of RSA, 40–49.

B. den Boer, A. Bosselaers, Collisions for the compression function of *MD5*, 293-304.

B. Dixon, A.K. Lenstra, Factoring integers using *SIMD* sieves, 28-39.

J. Domingo-Ferrer, Untransferable rights in a client-independent server environment, 260-266.

M. Jakobsson, Ripping coins for a fair exchange, 220-230.

A. Klapper, M. Goresky, Large period nearly de Bruijn FCSR sequences, 263-273.

K. Koyama, Fast RSA-type schemes based on singular cubic curves y^2 + axy $\equiv x^3$ (mod n), 329-340.

H. Krawczyk, New hash functions for message authentication, 301-3 10.

K. Kurosawa, S. Obana, Combinatorial bounds for authentication codes with arbitration, 289-300.

R. Lercier, F. Morain, Counting the number of points on elliptic curves over finite fields: strategies and performances, 79-94.

C.H. Lim, P.J. Lee, Server (prover/signer)-aided verification of identity proofs and signatures, 64-78.

PL. Montgomery, A block Lanczos algorithm for finding dependencies over $GF(2)$, 106-120.

D. Naccache, D. M'raïhi, W. Wolfowicz, A. di Porto, Are Crypto-accelerators really inevitable? 20 bit zero-knowledge in less than a second on simple *8-bit* microcontrollers, 404–409.

M. Näslund, Universal hash functions *&* hard core bits, 356-366.

L. O'Connor, Convergence in differential distributions, 13-23.

B. Pfitzmann, M. Schunter, M. Waidner, How to break another "provably *secure*" *payment* system, 121-132.

D. Pointcheval, A new identification scheme based on the *perceptrons* problem, 319-328.

K. Sako, J. Kilian, Receipt-free mix-type voting scheme – A practical solution to the implementation of a voting booth, 393-403.

K. Sakurai, H. Shizuya, Relationships among the computational powers of breaking discrete log *cryptosys*terns, 341-355.

C.P. Schnorr, H.H. Homer, Attacking the Char-Rivest cryptosystem by improved lattice reduction, 1-12.

M. Stadler, J.-M. Piveteau, J. Camenisch, Fair blind signatures, 209-219.

C.-H. Wang, T. Hwang, J.-J. Tsai, On the Matsumoto and Imai's human identification scheme, 382-392.

D. Weber, An implementation of the general number *field* sieve to compute discrete logarithms modp, 95–105.

X.-M. Zhang, Y. Zheng, On nonlinear resilient functions, 274-288.

Advances in Cryptology – **EUROCRYPT '96,** Zaragoza, Spain. Springer-Verlag LNCS 1070 (1996).
Editor: U.M. Maurer

W. Aiello, R. Venkatesan, Foiling birthday attacks in length-doubling transformations, 307-320.

D. Beaver, Equivocable oblivious transfer, 119-130.

M. Bellare, P. Rogaway, The exact security of digital signatures -how to sign with RSA and Rabin, 399-416.

S. Blackbum, M. Burrnester, Y. Desmedt, I? Wild, Efficient multiplicative sharing schemes, 107-l 18.

D. Bleichenbacher, Generating ElGamal signatures without knowing the secret key, 10-18.

J. Boyar, R. Peralta, Short discreet proofs, 13 1-142.

M. Burmester, Homomorphisms of secret sharing schemes: A tool for verifiable signature sharing, 96-106.

P. Camion, A. Canteaut, Constructions of t-resilient functions over a finite alphabet, 283-293.

D. Coppersmith, Finding a small root of a bivariate integer equation; factoring with high bits known, 178-189.

D. Coppersmith, Finding a small root of a univariate modular equation, 155-165.

D. Coppersmith, M. Franklin, J. Patarin, M. Reiter, Low-exponent RSA with related messages, 1-9.

R. Cramer, M. Franklin, B. Schoenmakers, M. Yung, Multi-authority secret-ballot elections with linear work, 72-83.

I.B. Damgård, T.P. Pedersen, New convertible undeniable signature schemes, 372-386.

J.-B. Fischer, J. Stem, An efficient pseudo-random generator provably as secure as syndrome decoding, 245–255.

R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, Robust threshold DSS signatures, 354-371.

K. Gibson, The security of the Gabidulin public key cryptosystem, 212-223.

J. Golić, Fast low order approximation of cryptographic functions, 268-282.

S.-M. Hong, S.-Y. Oh, H. Yoon, New modular multiplication algorithms for fast modular exponentiation, 166–177.

M. Jakobsson, K. Sako, R. Impagliazzo, Designated verifier proofs and their applications, 143-154.

J.D. Golić, L. O'Connor, Embedding and probabilistic correlation attacks on clock-controlled shift registers, 230-243.

M. Goresky, A. Klapper, Feedback registers based on ramified extensions of the 2-adic numbers, 215-222.

R. Göttfert, H. Niederreiter, A general lower bound for the linear complexity of the product of shift-register sequences, 223-229.

J. Hruby, Q-deformed quantum cryptography, 468–472.

M. Jakobsson, Blackmailing using undeniable signatures, 425–427.

T. Johansson, B. Smeets, On *A^2-codes* including arbiter's attacks, 456–460.

A. Joux, L. Granboulan, A practical attack against knapsack based hash functions, 58-66.

L.R. Knudsen, New potentially 'weak' keys for DES and *LOKI,* 419424.

L.R. Knudsen, X. Lai, New attacks on all double block length hash functions of hash rate 1, including the parallel-DM, 410–418.

C.-M. Li, T. Hwang, N.-Y. Lee, Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders, 194-204.

M. Matsui, On correlation between the order of S-boxes and the strength of DES, 366-375.

W. Meier, 0. Staffelbach, The self-shrinking generator, 205-214.

R. Menicocci, A systematic attack on clock controlled cascades, 450-455.

D. Naccache, D. M'Raïhi, S. Vaudenay, D. Raphaeli, Can D.S.A. be improved? Complexity trade-offs with the digital signature standard, 77-85.

M. Naor, A. Shamir, Visual cryptography, 1-12.

K. Nyberg, Linear approximation of block ciphers, 439–444.

K. Nyberg, R.A. Rueppel, Message recovery for signature schemes based on the discrete logarithm problem, 182-193.

G. Orton, A multiple-iterated trapdoor for dense compact knapsacks, 112-130.

B. Pfitzmann, Breaking an efficient anonymous channel, 332-340.

R. Safavi-Naini, L. Tombak, Authentication codes in plaintext and chosen-content attacks, 254-265.

C.P. Schnorr, S. Vaudenay, Black box cryptanalysis of hash networks based on multipermutations, 47-57.

J. Sebeny, X.-M. Zhang, Y. Zheng, Relationships among nonlinearity criteria, 376-388.

A. Shamir, Memory efficient variants ofpublic-key schemes for smart card applications, 445–449.

P. Syverson, C. Meadows, Formal requirements for key distribution protocols, 320-33 1.

R. Taylor, Near optimal unconditionally secure authentication, 244-253.

M. van Dijk, A linear construction of perfect secret sharing schemes, 23-34.

Y. Zheng, How to break and repair Leighton and Micah's key agreement protocol, 299-305.

Advances in Cryptology-EUROCRYPT '95, Saint-Malo, France. Springer-Verlag LNCS 921 (1995).
Editors: L.C. Guillou and J.-J. Quisquater

P. Béguin, A. Cresti, General short computational secret sharing schemes, 194-208.

J. Bierbrauer, *A^2-codes* from universal hash classes, 3 1 l-3 18.

S. Brands, Restrictive blinding of secret-key certificates, 231-247.

L. Chen, T.P. Pedersen, On the efficiency of group signatures providing information-theoretic anonymity, 39–49.

C. Crépeau, L. Salvail, Quantum oblivious mutual identification, 133-146.

S. D'Amiano, G. Di Crescenzo, Anonymous *NIZK proofs* ofknowledge with preprocessing, 413416.

Y. Desmedt, Securing traceability of ciphertexts – Towards a secure software key escrow system, 147-157.

G. Di Crescenzo, Recycling random bits in composed perfect zero-knowledge, 367-381.

M.K. Franklin, M.K. Reiter, Verifiable signature sharing, 50-63.

C. Gehrmann, Secure multiround authentication protocols, 158-167.

R. Gennaro, S. Micah, Verifiable secret sharing as secure computation, 168-182.

J.D. Golić, Towards fast correlation attacks on irregularly clocked shift registers, 248-262,

C. Harpes, G.G. Kramer, J.L. Massey, A generalization oflinearcryptanalysis and the *applicabilityofMatsui's* piling-up lemma, 24-38.

W.-A. Jackson, K.M. Martin, C.M. O'Keefe, Efficient secret sharing without a mutually trusted authority 183–193

Fast Software Encryption: Second International Workshop, Leuven, Belgium, December 1994.
Springer-Verlag LNCS 1008 (1995).
Editor: B. Preneel

R. Anderson, On Fibonacci keystream generators, 346-352.

R. Anderson, Searching for the optimum correlation attack, 137-143.

U. Baum, S. Blackburn, Clock-controlled pseudorandom generators on finite groups, 6-21.

E. Biham, P.C. Kocher, A known plaintext attack on the *PKZIP stream* cipher, 144–153.

M. Blaze, B. Schneier, The *MacGuffin* block cipher algorithm, 97-l 10.

U. Blöcher, M. Dichtl, Problems with the linear cryptanalysis of DES using more than one active S-box per round, 265-274.

W.G. Chambers, On random mappings and random permutations, 22-28.

J. Daemen, R. Govaerts, J. Vandewalle, Correlation matrices, 275-285.

C. Ding, Binary cyclotomic generators, 29-60.

H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, 61-74.

J.D. GoliC, Linear cryptanalysis of stream ciphers, 154-169.

B.S. Kaliski Jr., M.J.B. Robshaw, Linear cryptanalysis using multiple approximations and FEAL, 249-264.

A. Klapper, Feedback with carry shift registers over finite *fields*, 170-178.

L.R. Knudsen, Truncated and higher order differentials, 196211.

X. Lai, Additive and linear structures of cryptographic functions, 75-85.

S. Lucks, How to exploit the intractability of exact TSP for cryptography, 298-304.

D.J.C. MacKay, A free energy minimization framework for inference problems in modulo 2 arithmetic, 179-195.

J.L. Massey, SAFER K-64: One year later, 212-241.

K. Nyberg, S-boxes and round functions with controllable linearity and differential uniformity, 11 l-130.

L. O’Connor, Properties of linear approximation tables, 131-136.

W.T. Penzhorn, A fast homophonic coding algorithm based on arithmetic coding, 329-345.

B. Preneel, Introduction, l-5.

V. Rijmen, B. Preneel, Cryptanalysis of *McGuffin,* 353-358.

V. Rijmen, B. Preneel, Improved characteristics for differential cryptanalysis of hash functions based on block ciphers, 242-248.

R.L. Rivest, The RC5 encryption algorithm, 86-96.

M. Roe, How to reverse engineer an EES device, 305-328.

M. Roe, Performance of block ciphers and hash functions – one year later, 359-362.

S. Vaudenay, On the need for multipermutations: Cryptanalysis of MD4 and SAFER, 286-297.

D.J. Wheeler, R.M. Needham, TEA, a tiny encryption algorithm, 363-366.

Fast Software Encryption: Third International Workshop, Cambridge, UK., February 1996.
Springer-Verlag LNCS 1039 (1996).
Editor: D. Gollmann

R. Anderson, E. Biham, Tiger: a fast new hash function, 89-97.

R. Anderson, E. Biham, Two practical and provably secure block ciphers: BEAR and LION, 113-120.

M. Blaze, High-bandwidth encryption with low-bandwidth smartcards, 33-40.

A. Clark, J.D. Golić, E. Dawson, A comparison of fast correlation attacks, 145-157.

H. Dobbertin, Cryptanalysis of MD4, 53-69.

H. Dobbertin, A. Bosselaers, B. Preneel, *RIPEMD-160:* a strengthened version *of RIPEMD,* 71-82.

W. Geiselmann, A note on the hash function of *Tillich* and *Zémor,* 5 l-52.

J.D. Golić, On the security of nonlinear *filter* generators, 173-188.

R. Jenkins Jr., ISAAC, 41-49.

L.R. Knudsen, T.A. Berson, Truncated differentials of SAFER, 15-26.

A. Klapper, On the existence of secure feedback registers, 256-267.

L.R. Knudsen, T.P. Pedersen, On the difficulty of software key escrow, 237-244.

L.R. Knudsen, M.J.B. Robshaw, Non-linear approximations in linear cryptanalysis, 224-236.

B. Meyer, V. Miiller, A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring, 49-59.

W. Ogata, K. Kurosawa, Optimum secret sharing scheme secure against cheating, 200-211.

J. Patarin, Hidden fields equations *(HFE)* and isomotphisms of polynomials (IP): Two new families of asymmetric algorithms, 33-48.

B. Pfitzmann, M. Schunter, Asymmetric fingerprinting, 84-95.

D. Pointcheval, J. Stem, Security proofs for signature schemes, 387-398.

B. Preneel, P.C. van Oorschot, On the security of two MAC algorithms, 19-32.

F. Schwenk, J. Eisfeld, Public key encryption and signature schemes based on polynomials over $\mathbb{Z}_n$, 60-71.

V. Shoup, On the security of a practical identification scheme, 344-353.

V. Shoup, A. Rubin, Session key *distribution* using smart cards, 321-331.

M. Stadler, Publicly verifiable secret sharing, 190-199.

P.C. van Oorschot, M.J. Wiener, On Diffie-Hellman key agreement with short exponents, 332-343.

X.-M. Zhang, Y. Zheng, Auto-correlations and new bounds on the nonlinearity of Boolean functions, 294–306.

A.4 Fast Software Encryption Proceedings

Fast Software Encryption: Cambridge Security Workshop, Cambridge, UK., December 1993.
Springer-Verlag LNCS 809 (1994).
Editor: R. Anderson

R. Anderson, A modem rotor machine, 47–50.

E. Biham, On modes of operation, 116-120.

U. Blöcher, M. Dichtl, Fish: A fast software stream cipher, 41-44.

W.G. Chambers, Two stream ciphers, 5 l-55.

A. Chan, R. Games, J. Rushanan, On quadratic m-sequences, 166-173.

J. Daemen, R. Govaerts, J. Vandewalle, A new approach to block cipher design, 18-32.

A. Di Porto, W. Wolfowicz, *VINO:* A block cipher including variable permutations, 205-210.

C. Ding, The differential cryptanalysis and design of natural stream ciphers, 101-115.

J. Golić, On the security of shift register based keystream generators, 90-100.

D. Gollmann, Cryptanalysis of clock controlled shift registers, 121-126.

B.S. Kaliski Jr., M.J.B. Robshaw, Fast block cipher proposal, 33–40.

A. Klapper, M. Goresky, *2-Adic* shift registers, 174-178.

L.R. Knudsen, Practically secure Feistel ciphers, 211-221.

H. Krawczyk, The shrinking generator: Some practical considerations, 45–46.

X. Lai, L.R. Knudsen, Attacks on double block length hash functions, 157-165.

M. Lomas, Encrypting network traffic, 64-70.

N. Maclaren, Cryptographic pseudo-random numbers in simulation, 185-l 90.

J. Massey, SAFER K-64: A byte-oriented block-ciphering algorithm, 1-17.

K. Nyberg, New bent mappings suitable for fast implementation, 179-184.

B. Preneel, Design principles for dedicated hash functions, 71-82.

T. Renji, On finite automaton one-key cryptosystems, 135-148.

M. Roe, Performance of symmetric ciphers and one-way hash functions, 83-89.

P. Rogaway, D. Coppersmith, A software-optimized encryption algorithm, 56-63.

B. Schneier, Description of a new variable-length key, 64-bit block cipher (Blowfish), 191–204.

C. Schnorr, S. Vaudenay, Parallel m-hashing, 149-156.

D. Wheeler, A bulk data encryption algorithm, 127-134.

R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro, On the size of shares for secret sharing schemes, 6 (1993), 157-167.

D. Chaum, The dining cryptographers problem: Unconditional sender and recipient *untraceability,* 1 (1988), 65-75.

B. Chor, M. Geréb-Graus, E. Kushilevitz, On the structure of the privacy hierarchy, 7 (1994), 53-60.

B. Chor, E. Kushilevitz, Secret sharing over infinite domains, 6 (1993), 87-95.

D. Coppersmith, Modifications to the number field sieve, 6 (1993), 169-180.

Z.-D. Dai, Binary sequences derived from ML-Sequences over rings, I: Periods and minimal polynomials, 5 (1992), 193-207.

D.W. Davies, S. Murphy, Pairs and triplets of DES S-boxes, 8 (1995), l-25.

A. De Santis, G. Persiano, *The power* ofpreprocessing in zero-knowledge proofs ofknowledge, 9 (1996), 129–148.

M. De Soete, *New* bounds and constructions for authentication/secrecy codes with splitting, 3 (1991), 173–186.

M. Dyer, T. Fenner, A. Frieze, A. Thomason, On key storage in secure networks, 8 (1995), 189–200.

S. Even, 0. Goldreich, S. Micali, On-line/off-line digital signatures, 9 (1996), 35-67.

J.-H. Evertse, E. van Heyst, Which new RSA-signatures *can* be computed from certain given *RSA*-signatures?, 5 (1992), 41-52.

U. Feige, A. Fiat, A. Shamir, Zero-knowledge proofs of identity, 1 (1988), 77-94.

M. Fischer, R. Wright, Bounds on secret key exchange using a random deal of cards, 9 (1996), 71-99.

M.J. Fischer, S. Micali, C. Rackoff, A secure protocol for the oblivious transfer, 9 (1996), 191-195.

R. Forré, Methods and instruments for designing S-Boxes, 2 (1990), 115-130.

K. Gaarder, E. Snekkenes, Applying a formal analysis technique to the *CCITT X.509* strong two-way authentication protocol, 3 (1991), 81-98.

J. Georgiades, Some remarks on the security of the identification scheme based on permuted kernels, 5 (1992), 133-137.

P. Godlewski, C. Mitchell, Key-minimal cryptosystems for unconditional secrecy, 3 (1990), l-25.

0. Goldreich, A uniform-complexity treatment of encryption and zero-knowledge, 6 (1993), 21-53.

0. Goldreich, A. Kahan, How to construct constant-round zero-knowledgeproofsystems for NP, 9 (1996), 167-189.

0. Goldreich, E. Kushilevitz, A perfect zero-knowledge proof system for a problem equivalent to the discrete logarithm, 6 (1993), 97-116.

0. Goldreich, Y. Oren, Definitions and properties of zero-knowledge proof systems, 7 (1994), l-32.

J. Golić, Correlation properties of a general binary combiner with memory, 9 (1996), 111-126.

J. Golić, M. Mihaljević, A generalized correlation attack on a class of stream ciphers based on the *Leven*-shtein distance, 3 (1991), 201-212.

L. Gong, D.J. Wheeler, A matrix key-distribution scheme, 2 (1990), 51-59.

S. Haber, W.S. Stornetta, How to time-stamp a digital document, 3 (1991), 99-111.

H. Heys, S. Tavares, Substitution-permutation networks resistant to differential and linear *cryptanalysis,* 9 (1996), 1-19.

M. Ito, A. Saito, T. Nishizeki, Multiple assignment scheme for sharing secret, 6 (1993), 15-20.

T. Itoh, M. Hoshi, S. Tsujii, A low communication competitive interactive proof system for promised quadratic residuosity, 9 (1996), 101-109.

B.S. Kaliski Jr., One-way permutations on elliptic curves, 3 (1991), 187-199.

B.S. Kaliski Jr., R.L. Rivest, A.T. Sherman, *Is the* Data Encryption *Standard* a group? (Results of cycling experiments on DES), 1 (1988), 3-36.

R. Kemmerer, C. Meadows, J. Millen, Three systems for cryptographic protocol analysis, 7 (1994), 79-130.

A. Klapper, The vulnerability of geometric sequences based on fields of odd characteristic, 7 (1994), 33-51.

N. Koblitz, Hyperelliptic cryptosystems, 1 (1989), 139-150.

N. Koblitz, Elliptic curve implementation of zero-knowledge blobs, 4 (1991), 207-213.

A.K. Lenstra, Y. Yacobi, User impersonation in key certification schemes, 6 (1993), 225-232.

H.W. Lenstra Jr., On the Chor-Rivest knapsack cryptosystem, 3 (1991), 149-155.

S. Lloyd, Counting binary functions with certain cryptographic properties, 5 (1992), 107-131.

J.H. Loxton, D.S.P. Khoo, G.J. Bird, J. Seberry, A cubic RSA code equivalent to factorization, 5 (1992), 139–150.

M. Luby, C. Rackoff, A study ofpassword security, 1 (1989), 151-158.

S.S. Magliveras, N.D. Memon, Algebraic properties of cryptosystem PGM, 5 (1992), 167-183.

X. Lai, R.A. Rueppel, Attacks on the *HKM/HFX* cryptosystem, 1-14.

S. Lucks, Faster Luby-Rackoff ciphers, 189-203.

M. Matsui, New structure of block ciphers with provable security against differential and linear cryptanalysis, 205-218.

K. Nyberg, Fast accumulated hashing, 83-87.

W.T. Penzhorn, Correlation attacks on stream ciphers: computing low-weightparity checks based on error-correcting codes, 159-172.

V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, The cipher SHARK, 99-l 11.

B. Schneier, J. Kelsey, Unbalanced Feistel networks and block cipher design, 121-144.

S. Vaudenay, On the weak keys of Blowfish, 27-32.

A.5 Journal of Cryptology papers

Journal of Cryptology papers (Volume 1 No. 1 – Volume 9 No.3, 1988-l 996)

M. Abadi, J. Feigenbaum, Secure circuit evaluation, 2 (1990), I-12.

C. Adams, S. Tavares, The structured design of cryptographically good S-Boxes, 3 (1990), 27–41.

G.B. Agnew, T. Beth, R.C. Mullin, S.A. Vanstone, Arithmetic operations in $GF(2^m)$, 6 (1993), 3-13.

G.B. Agnew, R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, An implementation for a fast public-key cryptosystem, 3 (1991), 63-79.

P. Beauchemin, G. Brassard, A generalization of Hellman's extension to Shannon's approach to cryptography, 1 (1988), 129-131.

P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, C. Pomerance, The generation of random numbers that are probably prime, 1 (1988), 53-64.

D. Beaver, Secure multiparty protocols and zero-knowledge proof systems tolerating a faulty minority, 4 (1991), 75-122.

M. Bellare, M. Yung, Certifyingpermutations: Noninteractive zero-knowledge based on any trapdoor permutation, 9 (1996), 149-166.

I. Ben-Aroya, E. Biham, Differential cryptanalysis of Lucifer, 9 (1996), 21-34.

S. Bengio, G. Brassard, Y.G. Desmedt, C. Goutier, J.-J. Quisquater, Secure implementation of identification systems, 4 (1991), 175-183.

C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, Experimental quantum cryptography, 5 (1992), 3-28.

E. Biham, New types of cryptanalytic attacks using related keys, 7 (1994), 229-246.

E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, 4 (1991), 3-72.

S. Blackburn, S. Murphy, J. Stern, The cryptanalysis of a public-key implementation of finite group mappings, 8 (1995), 157-166.

C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro, Graph decompositions and secret sharing schemes, 8 (1995), 39-64.

J. Boyar, Inferring sequences produced by a linear congruential generator missing low-order bits, 1(1989), 177-184.

J. Boyar, K. Friedl, C. Lund, Practical zero-knowledge proofs: Giving hints and using deficiencies, 4 (1991), 185-206.

J. Boyar, C. Lund, R. Peralta, On the communication complexity of zero-knowledge proofs, 6 (1993), 65–85.

J.F. Boyar, S.A. Kurtz, M.W. Krentel, A discrete logarithm implementation of perfect zero-knowledge blobs, 2 (1990), 63-76.

E.F. Brickell, D.M. Davenport, On the classification of ideal secret sharing schemes, 4 (1991), 123-134.

E.F. Brickell, K.S. McCurley, An interactive identification scheme based on discrete logarithms and factoring, 5 (1992), 29-39.

E.F. Brickell, D.R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, 5 (1992), 153-166.

J. Buchmann, H.C. Williams, A key-exchange system based on imaginary quadratic fields, 1 (1988), 107-118.

References

[1] M. ABADI AND R. NEEDHAM, "Prudent engineering practice for cryptographic protocols", DEC SRC report #125, Digital Equipment Corporation, Palo Alto, CA, 1994.

[2] M. ABADI AND M.R. TUTTLE, "A semantics for a logic of authentication", Proceedings *of* the Tenth Annual ACM Symposium on Principles *of Distributed* Computing, 201-216, 1991.

[3] C. ADAMS, "Symmetric cryptographic system for data encryption", U.S. Patent # 5,511,123, 23 Apr 1996.

[4] ———, "IDUP and SPKM: Developing public-key-based APIs and mechanisms for communication security services", Proceedings *of* the Internet Society Symposium on Network and Distributed System Security, 128-135, IEEE Computer Society Press, 1996.

[5] C. ADAMS AND H. MEIJER, "Security-related comments regarding McEliece's public-key cryptosystem", Advances in Cryptology-CRYPTO '87 (LNCS *293)*, 224–228, 1988.

[6] ———, "Security-related comments regarding McEliece's public-key cryptosystem", IEEE Transactions on Information Theory, 35 (1989), 454-455. An earlier version appeared in [5].

[7] C. ADAMS AND S.E. TAVARES, "Designing S-boxes for ciphers resistant to differential cryptanalysis", W. Wolfowicz, editor, Proceedings *of* the 3rd Symposium on State and Progress *of* Research in Cryptography, Rome, Italy, 181-190, 1993.

[8] L.M. ADLEMAN, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography", Proceedings of the IEEE 20th Annual Symposium on Foundations *of* Computer Science, 55-60, 1979.

[9] ——— "The function field sieve", Algorithmic Number Theory (LNCS *877)*, 108-121, 1994.

[10] ———, "Molecular computation of solutions to combinatorial problems", Science, 266 (1994), 1021-1024.

[11] L.M. ADLEMAN AND J. DEMARRAIS, "A subexponential algorithm for discrete logarithms over all finite fields", Mathematics *of* Computation, 61 (1993), 1-15.

[12] L.M. ADLEMAN, J. DEMARRAIS, AND M.-D. HUANG, "A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields", Algorithmic Number Theory (LNCS *877)*, 28-40, 1994.

[13] L.M. ADLEMAN AND M.-D. A. HUANG, Primality Testing and *Abelian* Varieties Over Finite Fields, Springer-Verlag, Berlin, 1992.

[14] L.M. ADLEMAN AND H.W. LENSTRA JR., "Finding irreducible polynomials over finite fields", Proceedings *of* the 18th Annual ACM Symposium on Theory *of* Computing, 350–355, 1986.

[15] L.M. ADLEMAN AND K.S. MCCURLEY, "Open problems in number theoretic complexity, II", Algorithmic Number Theory (LNCS *877)*, 291-322, 1994.

[16] L.M. ADLEMAN, C. POMERANCE, AND R.S. RUMELY, "On distinguishing prime numbers from composite numbers", Annals *of* Mathematics, 117 (1983), 173-206.

[17] G.B. AGNEW, "Random sources for cryptographic systems", Advances in Cryptology-EUROCRYPT '87 (LNCS *304)*, 77-81, 1988.

[18] G.B. AGNEW, R.C. MULLIN, I.M. ONYSZCHUK, AND S.A. VANSTONE, "An implementation for a fast public-key cryptosystem", Journal *of* Cryptology, 3 (1991), 63-79.

193 G.B. AGNEW, R.C. MULLIN, AND S.A. VANSTONE, "Improved digital signature scheme based on discrete exponentiation", Electronics Letters, 26 (July 5, 1990), 1024-1025.

[20] S.G. AKL, "On the security of compressed encodings", Advances in Cryptology-Proceedings *of* Crypto 83, 209-230, 1984.

[21] N. ALEXANDRIS, M. BURMESTER, V. CHRISSIKOPOULOS, AND Y. DESMEDT, "A secure key distribution system", W. Wolfowicz,

S.M. Matyas, Keyprocessing with control vectors, 3 (1991), 113-136.

U. Maurer, Conditionally-perfect secrecy and a provably-secure randomized cipher, 5 (1992), 53-66.

U. Maurer, A universal statistical test for random bit generators, 5 (1992), 89–105.

U. Maurer, Fast generation of prime numbers and secure public-key cryptographic parameters, 8 (1995), 123-155.

U. Maurer, J.L. Massey, Local randomness in pseudorandom sequences, 4 (1991), 135-149.

U. Maurer, J.L. Massey, Cascade ciphers: The importance of being first, 6 (1993), 55-61.

K.S. McCurley, A key distribution system equivalent to factoring, 1 (1988), 95-105.

W. Meier, 0. Staffelbach, Fast correlation attacks on certain stream ciphers, 1 (1989), 159-176.

W. Meier, 0. Staffelbach, Correlation properties of combiners with memory in stream ciphers, 5 (1992), 67-86.

A. Menezes, S. Vanstone, Elliptic curve cryptosystems and their implementation, 6 (1993), 209-224.

R.C. Merkle, A fast software one-way hash function, 3 (1990), 43-58.

S. Micali, C.P. Schnorr, Efficient, perfect polynomial random number generators, 3 (1991), 157-l 72.

C. Mitchell, Enumerating Boolean functions of cryptographic significance, 2 (1990), 155-170.

S. Murphy, The cryptanalysis of FEAL-4 with 20 chosen plaintexts, 2 (1990), 145-154.

S. Murphy, K. Paterson, P. Wild, A weak cipher that generates the symmetric group, 7 (1994), 61-65.

M. Naor, Bit commitment usingpseudorandomness, 4 (1991), 151–158.

H. Niederreiter, A combinatorial approach to probabilistic results on the linear-complexity profile of random sequences, 2 (1990), 105-l 12.

K. Nishimura, M. Sibuya, Probability to meet in the middle, 2 (1990), 13-22.

K. Nyberg, L.R. Knudsen, Provable security against a differential attack, 8 (1995), 27-37.

L. O'Connor, An analysis of a class of algorithms for S-box construction, 7 (1994), 133-151.

L. O'Connor, On the distribution of characteristics in bijective mappings, 8 (1995), 67-86.

L. O'Connor, A. Klapper, Algebraic nonlinearity and its applications to cryptography, 7 (1994), 213-227.

G. Orton, L. Peppard, S. Tavares, A design of a fast pipelined modular multiplier based on a *diminished*-radix algorithm, 6 (1993), 183-208.

J. Pastor, CRYPTOPOST$^{\text{TM}}$-a cryptographic application to mail processing, 3 (1991), 137-146.

D. Pei, Information-theoretic bounds for authentication codes and block designs, 8 (1995), 177-l 88.

S.J. Phillips, N.C. Phillips, Strongly ideal secret sharing schemes, 5 (1992), 185-191.

F. Piper, M. Walker, Linear ciphers and spreads, 1 (1989), 185-188.

M. Qu, S.A. Vanstone, *Factorizations* in the elementary *abelian* p-group and their *cryptographic* significance, 7 (1994), 201-212.

U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages, 6 (1993), 135-156.

A. Russell, Necessary and sufficient conditions for collision-free hashing, 8 (1995), 87-99.

R. Scheidler, J.A. Buchmann, H.C. Williams, A key-exchange protocol using real quadratic fields, 7 (1994), 171-199.

C.P. Schnorr, Efficient signature generation by smart cards, 4 (1991), 161-174.

A.W. Schrift, A. Shamir, Universal tests for nonuniform distributions, 6 (1993), 119-133.

G.J. Simmons, A Cartesian product construction for unconditionally secure authentication codes that permit arbitration, 2 (1990), 77-104.

G.J. Simmons, Proof of soundness (integrity) of cryptographic protocols, 7 (1994), 69-77.

D.R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, 1 (1988), 119-127.

D.R. Stinson, Some constructions and bounds for authentication codes, 1 (1988), 37-51.

D.R. Stinson, The combinatorics of authentication and secrecy codes, 2 (1990), 23–49.

D.R. Stinson, J.L. Massey, An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions, 8 (1995), 167–173.

P. Syverson, Knowledge, belief and semantics in the analysis of cryptographic protocols, 1 (1992), 3 17-334.

S.-H. Teng, Functional inversion and communication complexity, 7 (1994), 153-170.

M. Tompa, H. Woll, How to share a secret with cheaters, 1 (1988), 133-138.

S.A. Vanstone, R.J. Zuccherato, Short RSA keys and their generation, 8 (1995), 101-114.

M. Walker, Information-theoretic bounds for authentication schemes, 2 (1990), 131-143.

Y.-X. Yang, B. Guo, Further enumerating boolean functions of cryptographic significance, 8 (1995), 115-122.

[44] ANSI X9.30 (PART 2), "American National Standard for Financial Services – Public key cryptography using irreversible algorithms for the financial services industry – Parr 2: The secure hash algorithm (SHA)", ASC X9 Secretariat – American Bankers Association, 1993.

[45] ANSI X9.31 (PART 1), "American National Standard for Financial Services – Public key cryptography using RSA for the financial services industry – Parr 1: The RSA signature algorithm", draft, 1995.

[46] ANSI X9.3 1 (PART 2), "American National Standard for Financial Services – Public key cryptography using RSA for the financial services industry – Parr 2: Hash algorithms for RSA", draft, 1995.

[47] ANSI X9.42, "Public key cryptography for the financial services industry: Management of symmetric algorithm keys using Diffie-Hellman", draft, 1995.

[48] ANSI X9.44, "Public key cryptography using reversible algorithms for the financial services industry: Transport of symmetric algorithm keys using RSA", draft, 1994.

[49] ANSI X9.45, "Public key cryptography for the financial services industry – Enhanced management controls using digital signatures and attribute certificates", draft, 1996.

[50] ANSI X9.52, "Triple data encryption algorithm modes of operation", draft, 1996.

[51] ANSI X9.55, "Public key cryptography for the financial services industry -Extensions to public key certificates and certificate revocation lists", draft, 1995.

[52] ANSI X9.57, "Public key cryptography for the financial services industry – Certificate management", draft, 1995.

[53] K. AOKI AND K. OHTA, "Differential-linear cryptanalysis of FEAL-8", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, E79-A (1996), 20-27.

[54] B. ARAZI, "Integrating a key distribution procedure into the digital signature standard", Electronics Letters, 29 (May 27, 1993), 966-967.

[55] ———, "On primality testing using purely divisionless operations", The Computer Journal, 37 (1994), 219-222.

[56] F. ARNAULT, "Rabin-Miller primality test: composite numbers which pass it", Mathematics *of* Computation, 64 (1995), 355-361.

[57] A.O.L. ATKIN AND R.G. LARSON, "On a primality test of Solovay and Strassen", SIAM Journal on Computing, 11 (1982), 789-79 1.

[58] A.O.L. ATKIN AND F. MORAIN, "Elliptic curves and primality proving", Mathematics *of* Computation, 61 (1993), 29-68.

[59] D. ATKINS, M. GRAFF, A.K. LENSTRA, AND P.C. LEYLAND, "The magic words are SQUEAMISH OSSIFRAGE", Advances in Cryptology-ASIACRYPT '94 (LNCS *917)*, 263-277, 1995.

[60] L. BABAI, 'Trading group theory for randomness", Proceedings *of* the 17th Annual ACM Symposium on Theory *of* Computing, 421-429, 1985.

[61] L. BABAI AND S. MORAN, "Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes", Journal *of* Computer and System Sciences, 36 (1988), 254-276.

[62] E. BACH, "Discrete logarithms and factoring", Report No. UCB/CSD 84/186, Computer Science Division (EECS), University of California, Berkeley, California, 1984.

[63] ———, Analytic Methods in the Analysis and Design *of* Number-Theoretic Algorithms, MIT Press, Cambridge, Massachusetts, 1985. An ACM Distinguished Dissertation.

[64] ———, "Explicit bounds for primality testing and related problems", Mathematics *of* Computation, 55 (1990), 355-380.

[65] ——— "Number-theoretic algorithms", Annual Review *of* Computer Science, 4 (1990), 119-172.

[66] ———, "Realistic analysis of some randomized algorithms", Journal *of* Computer and System Sciences, 42 (1991), 30-53.

[67] ———, "Toward a theory of Pollard's rho method", Information and Computation, 90 (1991), 139-155.

[68] E. BACH AND J. SHALLIT, "Factoring with cyclotomic polynomials", Proceedings *of* the IEEE 26th Annual Symposium on Foundations *of* Computer Science, 443–450, 1985.

[69] ———, "Factoring with cyclotomic polynomials", *Mathematics of* Computation, 52 (1989), 201-219. An earlier version appeared in [68].

editor, Proceedings of the 3rd Symposium on State and Progress *of* Research in Cryptography, Rome, Italy, 30-34, Feb. 1993.

[22] W. ALEXI, B. CHOR, 0. GOLDREICH, AND C.P. SCHNORR, "RSA/Rabin bits are $\frac{1}{2}$ + 1 */pol y* (log n) secure", Proceedings *of* the IEEE 25th Annual Symposium on Foundations *of* Computer Science, 449-457, 1984.

[23] ——, "RSA and Rabin functions: Certain parts are as hard as the whole", SIAM Journal on Computing, 17 (1988), 194-209. An earlier version appeared in [22].

[24] W.R. ALFORD, A. GRANVILLE, AND C. POMERANCE, "There are infinitely many Carmichael numbers", Annals *of* Mathematics, 140 (1994), 703-722.

[25] H. AMIRAZIZI AND M. HELLMAN, "Time-memory-processor trade-offs", IEEE Transactions on Information Theory, 34 (1988), 505-512.

[26] R. ANDERSON, "Practical RSA trapdoor", Electronics Letters, 29 (May 27, 1993), 995.

[27] ——, "The classification of hash functions", P.G. Farrell, editor, Codes and Cyphers: Cryptography and Coding IV, 83-93, Institute of Mathematics & Its Applications (IMA), 1995.

[28] ——, "On Fibonacci keystream generators", B. Preneel, editor, Fast *Software* Encryption, Second International Workshop (LNCS *1008)*, 346-352, Springer-Verlag, 1995.

[29] ——, "Searching for the optimum correlation attack", B. Preneel, editor, Fast *Software* Encryption, Second International Workshop (LNCS *1008)*, 137-143, Springer-Verlag, 1995.

[30] R. ANDERSON AND E. BIHAM, 'Two practical and provably secure block ciphers: BEAR and LION', D. Gollmann, editor, Fast Software Encryption, Third International Workshop (LNCS *1039)*, 113-120, Springer-Verlag, 1996.

[31] R. ANDERSON AND R. NEEDHAM, "Robustness principles for public key protocols", Advances in Cryptology-CRYPTO '9.5 (LNCS *963)*, 236-247, 1995.

[32] N.C. ANKENY, "The least quadratic non residue", Annals *of* Mathematics, 55 (1952), 65-72.

[33] ANSI X3.92, "American National Standard -Data Encryption Algorithm", American National Standards Institute, 1981.

[34] ANSI X3.106, "American National Standard for Information Systems – Data Encryption Algorithm – Modes of Operation", American National Standards Institute, 1983.

[35] ANSI X9.8, "American National Standard for Financial Services – Banking – Personal Identification Number management and security. Part 1: PIN protection principles and techniques; Part 2: Approved algorithms for PIN encipherment", ASC X9 Secretariat – American Bankers Association, 1995.

[36] ANSI X9.9 (REVISED), "American National Standard – Financial institution message authentication (wholesale)", ASC X9 Secretariat – American Bankers Association, 1986 (replaces X9.9-1982).

[37] ANSI X9.17, "American National Standard – Financial institution key management (wholesale)", ASC X9 Secretariat-American Bankers Association, 1985.

[38] ANSI X9.19, "American National Standard – Financial institution retail message authentication", ASC X9 Secretariat – American Bankers Association, 1986.

[39] ANSI X9.23, "American National Standard – Financial institution encryption of wholesale financial messages", ASC X9 Secretariat -American Bankers Association, 1988.

[40] ANSI X9.24, "American National Standard for Financial Services – Financial services retail key management", ASC X9 Secretariat – American Bankers Association, 1992.

[41] ANSI X9.26, "American National Standard – Financial institution sign-on authentication for wholesale financial transactions", ASC X9 Secretariat – American Bankers Association, 1990.

[42] ANSI X9.28, "American National Standard for Financial Services – Financial institution multiple center key management (wholesale)", ASC X9 Secretariat-American Bankers Association, 1991.

[43] ANSI X9.30 (PART 1), "American National Standard for Financial Services – Public key cryptography using irreversible algorithms for the financial services industry – Part 1: The digital signature algorithm (DSA)", ASC X9 Secretariat – American Bankers Association, 1995.

[93] M. BELLARE AND P. ROGAWAY, "Random oracles are practical: a paradigm for designing efficient protocols", Ist ACM Conference on Computer and Communications Security, 62-73, ACM Press, 1993.

[94] ——, "Entity authentication and key distribution", Advances in Cryptology-CRYPTO '93 (LNCS *773)*, 232-249, 1994.

[95] ——, "Optimal asymmetric encryption", Advances in Cryptology-EUROCRYPT '94 (LNCS *950)*, 92-l 11, 1995.

[96] ——,"Provably secure session key distribution – the three party case", Proceedings of the 27th Annual ACM Symposium on Theory of Computing, 57-66, 1995.

[97] M.J. BELLER, L.-F. CHANG, AND Y. YACOBI, "Privacy and authentication on a portable communications system", IEEE Global Telecommunications Conference, 1922-1927, 1991.

[98] ——, "Security for personal communications services: public-key vs. private key approaches", The Third IEEE International Symposium on Personal, Indoor and Mobile Radio Communications *(PIMRC'92)*, 26-3 1, 1992.

[99] ——, "Privacy and authentication on a portable communications system", IEEE Journal on Selected Areas in Communications, 11 (1993), 821-829.

[100] M.J. BELLER AND Y. YACOBI, "Minimal asymmetric authentication and key agreement schemes", October 1994 unpublished manuscript.

[101] ——,"Fully-fledged two-way public key authentication and key agreement for low-cost terminals", Electronics Letters, 29 (May 27, 1993), 999-1001.

[102] S.M. BELLOVIN AND M. MERRITT, "Cryptographic protocol for secure communications", U.S. Patent # 5,241,599, 31 Aug 1993.

[103] ——, "Limitations of the Kerberos authentication system", Computer Communication Review, 20 (1990), 119-132.

[104] ——, "Encrypted key exchange: password-based protocols secure against dictionary attacks", Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 72-84, 1992.

[105] ——, "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise", 1st ACM Conference on Computer and Communications Security, 244–250, ACM Press, 1993.

[106] ——, "An attack on the Interlock Protocol when used for authentication", IEEE Transactions on Information Theory, 40 (1994), 273-275.

[107] I. BEN-AROYA AND E. BIHAM, "Differential cyptanalysis of Lucifer", Advances in Cryptology-CRYPTO '93 (LNCS *773)*, 187–199, 1994.

[108] ——, "Differential cryptanalysis of Lucifer", Journal of Cryptology, 9 (1996), 21-34. An earlier version appeared in [107].

[109] M. BEN-OR, "Probabilistic algorithms in finite fields", Proceedings of the IEEE 22nd Annual Symposium on Foundations of Computer Science, 394-398, 1981.

[110] J. BENALOH, "Secret sharing homomorphisms: Keeping shares of a secret secret", Advances in Cryptology-CRYPTO '86 (LNCS *263)*, 251-260, 1987.

[111] J. BENALOH AND M. DE MARE, "One-way accumulators: A decentralized alternative to digital signatures", Advances in Cryptology-EUROCRYPT '93 (LNCS *765)*, 274-285, 1994.

[112] J. BENALOH AND J. LEICHTER, "Generalized secret sharing and monotone functions", Advances in Cryptology-CRYPTO '88 (LNCS *403)*, 27-35, 1990.

[113] S. BENGIO, G. BRASSARD, Y.G. DESMEDT, C. GOUTIER, AND J.-J. QUISQUATER, "Secure implementation of identification systems", Journal of Cryptology, 4 (1991), 175-183.

[114] C. BENNETT, G. BRASSARD, S. BREIDBART, AND S. WIESNER, "Quantum cryptography, or unforgeable subway tokens", Advances in Cryptology-Proceedings of Crypto *82*, 267–275, 1983.

[115] C. BENNETT, G. BRASSARD, AND A. EKERT, "Quantum cryptography", *Scientific* American, special issue (1997), 164-171.

[116] S. BERKOVITS, "How to broadcast a secret", Advances in Cryptology-EUROCRYPT *'91 (LNCS 547)*, 535-541, 1991.

[70] ——, *Algorithmic Number Theory, Volume I: Efficient Algorithms,* MIT Press, Cambridge, Massachusetts, 1996.

[71] E. BACH AND J. SORENSON, "Sieve algorithms for perfect power testing", *Algorithmica,* 9 (1993), 313-328.

[72] A. BAHREMAN, "PEMToolKit: Building a top-down certification hierarchy", *Proceedings of the Internet Society Symposium on Network and Distributed System Security,* 161-171, IEEE Computer Society Press, 1995.

[73] T. BARITAUD, M. CAMPANA, P. CHAUVAUD, AND H. GILBERT, "On the security of the permuted kernel identification scheme", *Advances in Cryptology-CRYPTO '92 (LNCS 740),* 305–311, 1993.

[74] W. BARKER, *Cryptanalysis of the Hagelin Cryptograph,* Aegean Park Press, Laguna Hills, California, 1977.

[75] P. BARRETT, "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor", *Advances in Cryptology-CRYPTO '86 (LNCS 263),* 31 l-323, 1987.

[76] R.K. BAUER, T.A. BERSON, AND R.J. FEIERTAG, "A key distribution protocol using event markers", *ACM Transactions on Computer Systems,* 1 (1983), 249-255.

[77] U. BAUM AND S. BLACKBURN, "Clock-controlled pseudorandom generators on finite groups", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008),* 6-21, Springer-Verlag. 1995.

[78] F. BAUSPIESS AND H.-J. KNOBLOCH, "How to keep authenticity alive in a computer network", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434), 38-46,* 1990.

[79] D. BAYER, S. HABER, AND W.S. STORNETTA, "Improving the efficiency and reliability of digital time-stamping", R. Capocelli, A. De Santis, and U. Vaccaro, editors, *Sequences II: Methods in Communication, Security, and Computer Science, 329-334,* Springer-Verlag, 1993.

[80] P. BEAUCHEMIN AND G. BRASSARD, "A generalization of Hellman's extension to Shannon's approach to cryptography", *Journal of Cryptology,* 1 (1988), 129-131.

[81] P. BEAUCHEMIN, G. BRASSARD, C. CRÉPEAU, C. GOUTIER, AND C. POMERANCE, "The generation of random numbers that are probably prime", *Journal of Cryptology,* 1 (1988), 53-64.

[82] P. BÉGUIN AND J.-J. QUISQUATER, "Secure acceleration of DSS signatures using insecure server", *Advances in Cryptology-ASIACRYPT '94 (LNCS 917). 249-259,* 1995.

[83] A. BEIMEL AND B. CHOR, "Interaction in key distribution schemes", *Advances in Cryptology-CRYPTO '93 (LNCS 773),* 444–455, 1994.

[84] H. BEKER AND F. PIPER, *Cipher Systems: The Protection of Communications,* John Wiley & Sons, New York, 1982.

[85] H. BEKER AND M. WALKER, "Key management for secure electronic funds transfer in a retail environment", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196),* 401410, 1985.

[86] M. BELLARE, R. CANETTI, AND H. KRAWCZYK, "Keying hash functions for message authenticaion", *Advances in Cryptology-CRYPTO '96 (LNCS 1109),* l-15,1996.

[87] M. BELLARE AND 0. GOLDREICH, "On defining proofs of knowledge", *Advances in Cryptology-CRYPTO '92 (LNCS 740), 390-*420, 1993.

[88] M. BELLARE, 0. GOLDREICH, AND S. GOLDWASSER, "Incremental cryptography: The case of hashing and signing", *Advances in Cryptology-CRYPTO '94 (LNCS 839),* 216-233, 1994.

[89] ——, "Incremental cryptography and application to virus protection", *Proceedings of the 27th Annual ACM Symposium on Theory of Computing, 45-56,* 1995.

[90] M. BELLARE, R. GUÉRIN, AND P. ROGAWAY, "XOR MACs: New methods for message authentication using finite pseudorandom functions", *Advances in Cryptology-CRYPTO '95 (LNCS 963),* 15-28, 1995.

[91] M. BELLARE, J. KILIAN, AND P. ROGAWAY, "The security of cipher block chaining", *Advances in Cryptology-CRYPTO '94 (LNCS 839),* 341-358, 1994.

[92] M. BELLARE AND S. MICALI, "How to sign given any trapdoor function", *Advances in Cryptology-CRYPTO '88 (LNCS 403), 200-*215, 1990.

[143] S. Blackburn, S. Murphy, and J. Stern, "The cryptanalysis of a public-key implementation of finite group mappings", *Journal of Cryptology, 8* (1995), 157-166.

[144] R.E. Blahut, *Principles and Practice of Information Theory*, Addison-Wesley, Reading, Massachusetts, 1987.

[145] I.F. Blake, R. Fuji-Hara, R.C. Mullin, and S.A. Vanstone, "Computing logarithms in finite fields of characteristic two", *SIAM Journal on Algebraic and Discrete Methods, 5* (1984), 276-285.

[146] I.F. Blake, S. Gao, and R. Lambert, "Constructive problems for irreducible polynomials over finite fields", T.A. Gulliver and N.P. Secord, editors, *Information Theory and Applications (LNCS 793), l-23,* Springer-Verlag, 1994.

[147] B. Blakley, G.R. Blakley, A.H. Chan, and J.L. Massey, 'Threshold schemes with disenrollment", *Advances in Cryptology-CRYPTO '92 (LNCS 740), 540-548,* 1993.

[148] G. Blakley, "Safeguarding cryptographic keys", *Proceedings of AFIPS National Computer Conference, 3* 13-317, 1979.

[149] ———, "A computer algorithm for calculating the product *AB* modulo *M*", *IEEE Transactions on Computers, 32* (1983), *497-500.*

[150] G. Blakley and I. Borosh, "Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages", *Computers and Mathematics with Applications,* 5:3 (1979), 169-178.

[151] G. Blakley and C. Meadows, "Security of ramp schemes", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196),* 242-268, 1985.

[152] M. Blaze, "Protocol failure in the escrowed encryption standard", *2nd ACM Conference on Computer and Communications Security,* 59-67, ACM Press, 1994.

[153] D. Bleichenbacher, "Generating ElGamal signatures without knowing the secret key", *Advances in Cryptology-EUROCRYPT* '96 *(LNCS 1070),* 10-18, 1996.

[154] D. Bleichenbacher, W. Bosma, and A.K. Lenstra, "Some remarks on Lucas-based cryptosystems", *Advances in Cryptology-CRYPTO '95 (LNCS 963),* 386–396, 1995.

[155] D. Bleichenbacher and U. Maurer, "Directed acyclic graphs, one-way functions and digital signatures", *Advances in Cryptology-CRYPTO '94 (LNCS 839),* 75–82, 1994.

[156] U. Blöcher and M. Dichtl, "Fish: A fast software stream cipher", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809),* 41–44, Springer-Verlag, 1994.

[157] R. Blom, "Non-public key distribution", *Advances in Cryptology-Proceedings of Crypto 82,* 23 l-236, 1983.

158] ———, "An optimal class of symmetric key generation systems", *Advances in Cryptology-Proceedings of EUROCRYPT 84 (LNCS 209), 335-338,* 1985.

[159] L. Blum, M. Blum, and M. Shub, "Comparison of two pseudo-random number generators", *Advances in Cryptology-Proceedings of Crypto 82,* 61–78, 1983.

[160] ———, "A simple unpredictable pseudo-random number generator", *SIAM Journal on Computing,* 15 (1986), 364-383. An earlier version appeared in [159].

[161] M. Blum, "Independent unbiased coin flips from a correlated biased source: a finite state Markov chain", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science,* 425–433, 1984.

[162] M. Blum, A. De Santis, S. Micali, and G. Persiano, "Noninteractive zero-knowledge", *SIAM Journal on Computing, 20* (1991), 1084-1118.

[163] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications", *Proceedings of the 20th Annual ACM Symposium on Theory of Computing,* 103-112, 1988.

[164] M. Blum and S. Goldwasser, "An efficient probabilistic public-key encryption scheme which hides all partial information", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196), 289-299,* 1985.

[165] M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudo random bits", *Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science,* 112-117, 1982.

[166] ———, "How to generate cryptographically strong sequences of pseudo-random bits",

[117] E.R. BERLEKAMP, "Factoring polynomials over finite fields", *Bell System Technical Journal, 46* (1967), 1853-1859.

[118] ——, *Algebric Coding Theory,* McGraw Hill, New York, 1968.

[119] ——, "Factoring polynomials over large finite fields", *Mathematics of Computation, 24* (1970), 713-735.

[120] E.R. BERLEKAMP, R.J. MCELIECE, AND H.C.A. VAN TILBORG, "On the inherent intractability of certain coding problems", *IEEE Transactions on Information Theory, 24* (1978), 384-386.

[121] D.J. BERNSTEIN, "Detecting perfect powers in essentially linear time", preprint, 1995.

[122] D.J. BERNSTEIN AND A.K. LENSTRA, "A general number field sieve implementation", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve,* volume 1554 of *Lecture Notes in Mathematics,* 103-126, Springer-Verlag, 1993.

[123] T. BETH, "Efficient zero-knowledge identification scheme for smart cards", *Advances in Cryptology-EUROCRYPT '88 (LNCS 330),* 77-84, 1988.

[124] T. BETH AND Z.-D. DAI, "On the complexity of pseudo-random sequences – or: If you can describe a sequence it can't be random", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434), 533-543,* 1990.

[125] T. BETH, H.-J. KNOBLOCH, M. OTTEN, G.J. SIMMONS, AND P. WICHMANN, "Towards acceptable key escrow systems", *2nd ACM Conference on Computer and Communications Security,* 51-58, ACM Press, 1994.

[126] T. BETH AND F.C. PIPER, "The stop-and-go generator", *Advances in Cryptology-Proceedings of EUROCRYPT84 (LNCS 209),* 88-92, 1985.

[127] J. BIERBRAUER, T. JOHANSSON, G. KABATIANSKII, AND B. SMEETS, "On families of hash functions via geometric codes and concatenation", *Advances in Cryptology-CRYPTO '93 (LNCS 773),* 331-342, 1994.

[128] E. BIHAM, "New types of cryptanalytic attacks using related keys", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765),* 398409, 1994.

[129] ——, "New types of cryptanalytic attacks using related keys", *Journal of Cryptology, 7* (1994), 229-246.

[130] ——, "On modes of operation", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809),* 116–120, Springer-Verlag. 1994.

[131] ——, "Cryptanalysis of multiple modes of operation", *Advances in Cryptology-ASIACRYPT '94 (LNCS 917),* 278–292, 1995.

[132] ——, "On Matsui's linear cryptanalysis", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950),* 341-355, 1995.

[133] E. BIHAM AND A. BIRYUKOV, "How to strengthen DES using existing hardware", *Advances in Cryptology-ASIACRYPT '94 (LNCS 917),* 398–412, 1995.

[134] E. BIHAM AND A. SHAMIR, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology, 4* (1991), 3-72. An earlier version appeared in [135].

[135] ——, "Differential cryptanalysis of DES-like cryptosystems", *Advances in Cryptology-CRYPTO '90 (LNCS 537), 2-21, 1991.*

[136] ——, "Differential cryptanalysis of Feal and N-Hash", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547),* 1-16, 1991.

[137] ——, "Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI, and Lucifer", *Advances in Cryptology-CRYPTO '91 (LNCS 576),* 156-171, 1992.

[138] ——, *Differential Cryptanalysis of the Data Encryption Standard,* Springer-Verlag, New York, 1993.

[139] ——, "Differential cryptanalysis of the full 16-round DES", *Advances in Cryptology–CRYPTO '92 (LNCS 740), 487-496,* 1993.

[140] R. BIRD, I. GOPAL, A. HERZBERG, P. JANSON, S. KUTTEN, R. MOLVA, AND M. YUNG, "Systematic design of two-party authentication protocols", *Advances in Cryptology-CRYPTO '91 (LNCS 576),* 44–61, 1992.

[141] ——, "Systematic design of a family of attack-resistant authentication protocols", *IEEE Journal on Selected Areas in Communications,* 11 (1993), 679-693.

[142] ——, 'The KryptoKnight family of lightweight protocols for authentication and key distribution", *IEEE/ACM Transactions on Networking, 3* (1995), 31-41.

[190] G. Brassard, "A note on the complexity of cryptography", *IEEE Transactions on Information Theo y, 25* (1979), 232-233.

[191] ———, "On computationally secure authentication tags requiring short secret shared keys", *Advances in C yptology-Proceedings of Crypto 82*, 79–86, 1983.

[192] ———, *Modem Cryptology: A Tutorial*, LNCS 325, Springer-Verlag, New York, 1988.

[193] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge", *Journal of Computer and System Sciences, 37* (1988), 156-189.

[194] G. Brassard and C. Crépeau, "Zero-knowledge simulation of Boolean circuits", *Advances in Cryptology-CRYPTO '86 (LNCS 263)*, 223-233, 1987.

[195] ———, "Sorting out zero-knowledge", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434)*, 181-191, 1990.

[196] R.P. Brent, "An improved Monte Carlo factorization algorithm", *BIT, 20* (1980), 176–184.

[197] R.P. Brent and J.M. Pollard, "Factorization of the eighth Fermat number", *Mathematics of Computation, 36* (1981), 627–630.

[198] D.M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, New York, 1989.

[199] E.F. Brickell, "A fast modular multiplication algorithm with applications to two key cryptography", *Advances in Cyptology-Proceedings of Crypto 82*, 51–60, 1983.

[200] "Breaking iterated knapsacks", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196), 342-358,* 1985.

[201] ———, "The cryptanalysis of knapsack cryptosystems", R.D. Ringeisen and ES. Roberts, editors, *Applications of Discrete Mathematics, 3-23,* SIAM, 1988.

[202] E.F. Brickell and J.M. DeLaurentis, "An attack on a signature scheme proposed by Okamoto and Shiraishi", *Advances in Cryptology-CRYPTO '85 (LNCS 218), 28-*32, 1986.

[203] E.F. Brickell, D.M. Gordon, and K.S. McCurley, "Method for exponentiating in cryptographic systems", U.S. Patent # 5,299,262, 29 Mar 1994.

[204] E.F. Brickell, D.M. Gordon, K.S. McCurley, and D.B. Wilson, "Fast exponentiation with precomputation", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658)*, 200-207, 1993.

[205] E.F. Brickell, P.J. Lee, and Y. Yacobi, "Secure audio teleconference", *Advances in Cryptology-CRYPTO '87 (LNCS 293)*, 418-426, 1988.

[206] E.F. Brickell and K.S. McCurley, "An interactive identification scheme based on discrete logarithms and factoring", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473)*, 63-71, 1991.

[207] ———, "An interactive identification scheme based on discrete logarithms and factoring", *Journal of Cryptology, 5* (1992), 29-39. An earlier version appeared in [206].

[208] E.F. Brickell and A.M. Odlyzko, "Cryptanalysis: A survey of recent results", *Proceedings of the IEEE, 76* (1988), 578-593.

[209] ———, "Cryptanalysis: A survey of recent results", G.J. Simmons, editor, *Contempora y Cryptology: The Science of Information Integrity,* 501-540, IEEE Press, 1992. An earlier version appeared in [208].

[210] J. Brillhart, D. Lehmer, and J. Selfridge, "New primality criteria and factorizations of $2^m \pm 1$", *Mathematics of Computation, 29* (1975), 620-647.

[211] J. Brillhart, D. Lehmer, J. Selfridge, B. Tuckerman, and S. Wagstaff Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers,* volume *22* of *Contemporary Mathematics,* American Mathematical Society, Providence, Rhode Island, 2nd edition, 1988.

[212] J. Brillhart and J. Selfridge, "Some factorizations of $2^n \pm 1$ and related results", *Mathematics of Computation,* 21 (1967), 87-96.

[213] D. Brillinger, *Time Series: Data Analysis and Theory,* Holden-Day, San Francisco, 1981.

[214] L. Brown, M. Kwan, J. Pieprzyk, and J. Seberry, "Improving resistance to differential cryptanalysis and the redesign of LOKI", *Advances in Cyptology-ASIACRYPT '91 (LNCS 739)*, 36–50, 1993.

[215] L. Brown, J. Pieprzyk, and J. Seberry, "LOKI -a cryptographic primitive for authentication and secrecy applications", *Advances*

SIAM Journal on Computing, 13 (1984), 850–864. An earlier version appeared in [165].

[167] C. BLUNDO AND A. CRESTI, "Space requirements for broadcast encryption", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950)*, 287-298, 1995.

[168] C. BLUNDO, A. CRESTI, A. DE SANTIS, AND U. VACCARO, "Fully dynamic secret sharing schemes", *Advances in Cryptology-CRYPTO* '93 *(LNCS 773)*, 110-125, 1994.

[169] C. BLUNDO, A. DE SANTIS, A. HERZBERG, S. KUTTEN, U. VACCARO, AND M. YUNG, "Perfectly-secure key distribution for dynamic conferences", *Advances in Cryptology-CRYPTO '92 (LNCS 740)*, 471-486, 1993.

[170] R.V. BOOK AND F. OTTO, "The verifiability of two-party protocols", *Advances in Cryptology-EUROCRYPT '8.5 (LNCS 219)*, 254-260, 1986.

[171] A. BOOTH, "A signed binary multiplication technique", *The Quarterly Journal of Mechanics and Applied Mathematics, 4* (195 1), 236-240.

[172] J. BOS AND D. CHAUM, "Provably unforgeable signatures", *Advances in Cryptology-CRYPTO '92 (LNCS 740)*, 1-14, 1993.

[173] J. BOS AND M. COSTER, "Additon chain heuristics", *Advances in Cryptology-CRYPTO '89 (LNCS 435), 400-407,* 1990.

[174] W. BOSMA AND M.-P VAN DER HULST, "Faster primality testing", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434)*, 652-656, 1990.

[175] A. BOSSELAERS, R. GOVAERTS, AND J. VANDEWALLE, "Cryptography within phase I of the EEC-RACE programme", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 227-234, Springer-Verlag, 1993.

[176] —— "Comparison of three modular reductioh functions", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 175-186, 1994.

[177] ——, "Fast hashing on the Pentium", *Advances in Cryptology-CRYPTO '96 (LNCS 1109)*, 298-312, 1996.

[178] A. BOSSELAERS AND B. PRENEEL, editors, *Integrity Primitives for Secure Information Systems: Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040,* LNCS 1007, Springer-Verlag, New York, 1995.

[179] J . B OYAR, "Inferring sequences produced by a linear congmential generator missing low-order bits", *Journal of Cryptology,* 1 (1989), 177-184.

[180] - , "Inferring sequences produced by pseudo-random number generators", *Journal of the Association for Computing Machinery,* 36 (1989), 129-141.

[181] J. BOYAR, D. CHAUM, I.B. DAMGÅRD, AND T. PEDERSEN, "Convertible undeniable signatures", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 189-205, 1991.

[182] C. BOYD, "Digital multisignatures", H. Beker and F. Piper, editors, *Cryptography and Coding,* Institute of Mathematics & Its Applications (IMA), 241-246, Clarendon Press, 1989.

[183] C. BOYD AND W. MAO, "On a limitation of BAN logic", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765)*, 240–247, 1994.

[184] B.O. BRACHTL, D. COPPERSMITH, M.M. HYDEN, S.M. MATYAS JR., C.H.W. MEYER, J. OSEAS, S. PILPEL, AND M. SCHILLING, "Data authentication using modification detection codes based on a public one-way encryption function", U.S. Patent # 4,908,861, 13 Mar 1990.

[185] S. BRANDS, "Restrictive blinding of secret-key certificates", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921)*, 231-247, 1995.

[186] J. BRANDT AND I. DAMGÅRD, "On generation of probable primes by incremental search", *Advances in Cryptology-CRYPTO* '92 *(LNCS 740), 358-370,* 1993.

[187] J. BRANDT, I. DAMGÅRD, AND P. LANDROCK, "Speeding up prime number generation", *Advances in Cryptology-ASIACRYPT '91 (LNCS 739)*, 440–449, 1993.

[188] J. BRANDT, I. DAMGÅRD, P. LANDROCK, AND T. PEDERSEN, "Zero-knowledge authentication scheme with secret key exchange", *Advances in Cryptology-CRYPTO* '88 *(LNCS 403), 583-588,* 1990.

[189] D.K. BRANSTAD, "Encryption protection in computer data communications", *Proceedings of the 4th Data Communications Symposium* (Quebec), 8.1-8.7, IEEE, 1975.

[240] B. CHAR, K. GEDDES, G. GONNET, B. LEONG, M. MONAGAN, AND S. WATT, *Maple V Library Reference Manual,* Springer-Verlag, New York, 199 1.

[241] C. CHARNES, L. O'CONNOR, J. PIEPRZYK, R. SAFAVI-NAINI, AND Y. ZHENG, "Comments on Soviet encryption algorithm", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950),* *433-438,* 1995.

[242] D. CHAUM, "Blind signatures for untraceable payments", *Advances in Cryptology-Proceedings of Crypto 82,* 199-203, 1983.

[243] ———, "Security without identification: transaction systems to make big brother obsolete", *Communications of the ACM, 28* (1985), 1030-1044.

[244] ———, "Demonstrating that a public predicate can be satisfied without revealing any information about how", *Advances in Cryptology-CRYPTO '86 (LNCS 263),* 195–199, 1987.

[245] ———, "Blinding for unanticipated signatures", *Advances in Cryptology-EUROCRYPT* '87 *(LNCS 304), 227-233,* 1988.

[246] ———, "Zero-knowledge undeniable signatures", *Advances in Cryptology-EUROCRYPT* '90 *(LNCS 473),* 458–464, 199 1.

[247] ———, "Designated confirmer signatures", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950),* 86-91, 1995.

[248] D. CHAUM, J.-H. EVERTSE, AND J. VAN DE GRAAF, "An improved protocol for demonstrating possession of discrete logarithms and some generalizations", *Advances in Cryptology-EUROCRYPT '87 (LNCS 304),* 127-141, 1988.

[249] D. CHAUM, J.-H. EVERTSE, J. VAN DE GRAAF, AND R. PERALTA, "Demonstrating possession of a discrete logarithm without revealing it", *Advances in Cryptology-CRYPTO* '86 *(LNCS 263),* 200-212, 1987.

[250] D. CHAUM, A. FIAT, AND M. NAOR, "Untraceable electronic cash", *Advances in Cryptology-CRYPTO '88 (LNCS 403),* 319-327, 1990.

[251] D. CHAUM AND T.P. PEDERSEN, "Wallet databases with observers", *Advances in Cryptology-CRYPTO '92 (LNCS 740), 89-*105, 1993.

[252] D. CHAUM AND H. VAN ANTWERPEN, "Undeniable signatures", *Advances in Cryptology-CRYPTO '89 (LNCS 435), 2* 12–216, 1990.

[253] D. CHAUM, E. VAN HEIJST, AND B. PFITZMANN, "Cryptographically strong undeniable signatures, unconditionally secure for the signer", *Advances in Cryptology-CRYPTO '91 (LNCS 576),* 470–484, 1992.

[254] D. CHAUM AND E. VAN HEYST, "Group signatures", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547), 257-265,* 1991.

[255] L. CHEN AND T.P. PEDERSEN, "New group signature schemes", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950),* 171-181, 1995.

[256] V. CHEPYZHOV AND B. SMEETS, "On a fast correlation attack on certain stream ciphers", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547),* 176-185, 1991.

[257] B. CHOR AND 0. GOLDREICH, "Unbiased bits from sources of weak randomness and probabilistic communication complexity", *Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science,* 429–442, 1985.

[258] ———, "Unbiased bits from sources of weak randomness and probabilistic communication complexity", *SIAM Journal on Computing,* 17 (1988), 230-261. An earlier version appeared in [257].

[259] B. CHOR, S. GOLDWASSER, S. MICALI, AND B. AWERBUCH, "Verifiable secret sharing and achieving simultaneity in the presence of faults", *Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science, 383-395,* 1985.

[260] B. CHOR AND R.L. RIVEST, "A knapsack type public key cryptosystem based on arithmetic in finite fields", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196), 54-65,* 1985.

[261] ———, "A knapsack-type public key cryptosystem based on arithmetic in finite fields", *IEEE Transactions on Information Theory, 34* (1988), 901-909. An earlier version appeared in [260].

[262] A. CLARK, J. GOLIĆ, AND E. DAWSON, "A comparison of fast correlation attacks", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039),* 145-157, Springer-Verlag. 1996.

in Cryptology-AUSCRYPT '90 (LNCS 453), 229–236, 1990.

[216] J. BUCHMANN AND S. DÜLLMANN, "On the computation of discrete logarithms in class groups", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 134-139, 1991.

[217] J. BUCHMANN, J. LOHO, AND J. ZAYER, "An implementation of the general number field sieve", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 159-l 65, 1994.

[218] J. BUCHMANN AND H.C. WILLIAMS, "A key-exchange system based on imaginary quadratic fields", *Journal of Cryptology*, 1 (1988), 107-118.

[219] J.P. BUHLER, H.W. LENSTRA JR., AND C. POMERANCE, "Factoring integers with the number field sieve", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics, 50-94*, Springer-Verlag, 1993.

[220] M. BURMESTER, "On the risk of opening distributed keys", *Advances in Cryptology-CRYPTO '94 (LNCS 839)*, 308-317, 1994.

[221] M. BURMESTER AND Y. DESMEDT, "Remarks on soundness of proofs", *Electronics Letters, 25* (October 26, 1989), 1509-1511.

[222] ———, "A secure and efficient conference key distribution system", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950)*, 275–286, 1995.

[223] M. BURMESTER, Y. DESMEDT, F. PIPER, AND M. WALKER, "A general zero-knowledge scheme", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434)*, 122-133, 1990.

[224] M. BURROWS, M. ABADI, AND R. NEEDHAM, "A logic of authentication", *Proceedings of the Royal Society of London Series A: Mathematical and Physical Sciences, 246* (1989), 233-271. Preliminary version appeared as 1989 version of [227].

[225] ———, "A logic of authentication", *Proceedings of the 12th Annual ACM Symposium on Operating Systems Principles*, 1-13, 1989.

[226] ———, "A logic of authentication", *ACM Transactions on Computer Systems, 8* (1990), 18-36.

[227] ———, "A logic of authentication", DEC SRC report #39, Digital Equipment Corporation, Palo Alto, CA, Feb. 1989. Revised Feb. 1990.

[228] J.L. CAMENISCH, J.-M. PIVETEAU, AND M.A. STADLER, "Blind signatures based on the discrete logarithm problem", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950)*, 428–432, 1995.

[229] K.W. CAMPBELL AND M.J. WIENER, "DES is not a group", *Advances in Cryptology-CRYPTO '92 (LNCS 740)*. 512–520, 1993.

[230] C.M. CAMPBELL JR., "Design and specification of cryptographic capabilities", D.K. Branstad, editor, *Computer security and the Data Encryption Standard, 54-66*, NBS Special Publication 500-27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.

[231] E.R. CANFIELD, P. ERDÖS, AND C. POMERANCE, "On a problem of Oppenheim concerning 'Factorisatio Numerorum"', *Journal of Number Theory*, 17 (1983), l-28.

[232] D.G. CANTOR AND H. ZASSENHAUS, "A new algorithm for factoring polynomials over finite fields", *Mathematics of Computation, 36* (1981), 587–592.

[233] J.L. CARTER AND M.N. WEGMAN, "Universal classes of hash functions", *Proceedings of the 9th Annual ACM Symposium on Theory of Computing*, 106-l 12, 1977.

[234] ———, "Universal classes of hash functions", *Journal of Computer and System Sciences*, 18 (1979), 143–154. An earlier version appeared in [233].

[235] F. CHABAUD, "On the security of some cryptosystems based on error-correcting codes", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950)*, 131-139, 1995.

[236] G. J. CHAITIN, "On the length of programs for computing finite binary sequences", *Journal of the Association for Computing Machinery*, 13 (1966), 547–569.

[237] W.G. CHAMBERS, "Clock-controlled shift registers in binary sequence generators", *IEE Proceedings E – Computers and Digital Techniques*, 135 (1988), 17-24.

[238] ———, "Two stream ciphers", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 5 1–55, Springer-Verlag, 1994.

[239] W.G. CHAMBERS AND D. GOLLMANN, "Lock-in effect in cascades of clock-controlled shift-registers", *Advances in Cryptology-EUROCRYPT '88 (LNCS 330)*, 331–343, 1988.

[289] J. DAEMEN, *Cipher and hash function design*, PhD thesis, Katholieke Universiteit Leuven (Belgium), 1995.

[290] J. DAEMEN, R. GOVAERTS, AND J. VANDEWALLE, "A new approach to block cipher design", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 18-32, Springer-Verlag, 1994.

[291] ———, "Resynchronization weaknesses in synchronous stream ciphers", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765)*, 159–167, 1994.

[292] ———, "Weak keys for IDEA", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 224–231, 1994.

[293] Z.-D DAI, "Proof of Rueppel's linear complexity conjecture", *IEEE Transactions on Information Theory, 32* (1986), 440–443.

[294] Z.-D. DAI AND J.-H. YANG, "Linear complexity of periodically repeated random sequences", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547)*, 168-175, 1991.

[295] I.B. DAMGÅRD, "Collision free hash functions and public key signature schemes", *Advances in Cryptology-EUROCRYPT '87 (LNCS 304)*, 203-216, 1988.

[296] ———, "A design principle for hash functions", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 416-427, 1990.

[297] ———, "Towards practical public key systems secure against chosen ciphertext attacks", *Advances in Cryptology-CRYPTO '91 (LNCS 576)*, 445–456, 1992.

[298] ———, "Practical and provably secure release of a secret and exchange of signatures", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765)*, 200-217, 1994.

[299] I.B. DAMGÅRD AND P. LANDROCK, "Improved bounds for the Rabin primality test", M.J. Ganley, editor, *Cryptography and Coding III*, volume 45 of *Institute of Mathematics & Its Applications (IMA)*, 117-128, Clarendon Press, 1993.

[300] I.B. DAMGÅRD, P. LANDROCK, AND C. POMERANCE, "Average case error estimates for the strong probable prime test", Mathematics *of Computation*, 61 (1993), 177-194.

[301] H. DAVENPORT, "Bases for finite fields", *The Journal of the London Mathematical Society*, 43 (1968), 21-39.

[302] G.I. DAVIDA, "Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem", Technical Report TR-CS-82-2, Department of Electrical Engineering and Computer Science, University of Wisconsin, Milwaukee, WI, 1982.

[303] D.W. DAVIES, "Some regular properties of the 'Data Encryption Standard' algorithm", *Advances in Cryptology-Proceedings of Crypto 82*, 89–96, 1983.

[304] ———, "A message authenticator algorithm suitable for a mainframe computer", Advances *in Cryptology-Proceedings of CRYPTO 84 (LNCS 196)*, 393–400, 1985.

[305] ———, "Schemes for electronic funds transfer at the point of sale", K.M. Jackson and J. Hruska, editors, *Computer Security Reference Book, 667-689*, CRC Press, 1992.

[306] D.W. DAVIES AND D.O. CLAYDEN, "The message authenticator algorithm (MAA) and its implementation", Report DITC 109/88, National Physical Laboratory, U.K., February 1988.

[307] D.W. DAVIES AND G.I.P. PARKIN, "The average cycle size of the key stream in output feedback encipherment", *Advances in Cryptology-Proceedings of Crypto 82*, 97–98, 1983.

[308] D.W. DAVIES AND W.L. PRICE, *Security for Computer Networks*, John Wiley & Sons, New York, 2nd edition, 1989.

[309] D. DAVIS, R. IHAKA, AND P. FENSTERMACHER, "Cryptographic randomness from air turbulence in disk drives", *Advances in Cryptology-CRYPTO '94 (LNCS 839)*, 114–120, 1994.

[310] D. DAVIS AND R. SWICK, "Network security via private-key certificates", *Operating Systems Review, 24* (1990), 64-67.

[311] J.A. DAVIS, D.B. HOLDRIDGE, AND G.J. SIMMONS, "Status report on factoring (at the Sandia National Labs)", *Advances in Cryptology-Proceedings of EUROCRYPT 84 (LNCS 209)*, 183-215, 1985.

[312] E. DAWSON, "Cryptanalysis of summation generator", Advances *in Cryptology-AUSCRYPT '92 (LNCS 718), 209-215*, 1993.

[263] H. COHEN, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.

[264] H. COHEN AND A.K. LENSTRA, "Implementation of a new primality test", *Mathematics of Computation*, 48 (1987), 103-121.

[265] H. COHEN AND H.W. LENSTRA JR., "Primality testing and Jacobi sums", *Mathematics of Computation, 42* (1984), 297-330.

[266] D. COPPERSMITH, "Fast evaluation of logarithms in fields of characteristic two", *IEEE Transactions on Information Theory, 30* (1984), 587-594.

[267] ——— "Another birthday attack", *Advances in Cryptology-CRYPTO '85 (LNCS 218)*, 14-17, 1986.

[268] ———, "The real reason for Rivest's phenomenon", *Advances in Cryptology-CRYPTO '8.5 (LNCS 218), 535-536,* 1986.

[269] ———, "Modifications to the number field sieve", *Journal of Cryptology, 6* (1993), 169-180.

[270] ———, "Solving linear equations over $GF(2)$: Block Lanczos algorithm", *Linear Algebra and its Applications,* 192 (1993), 33-60.

[271] ———, "The Data Encryption Standard (DES) and its strength against attacks", *IBM Journal of Research and Development, 38* (1994), 243-250.

[272] ——— "Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm", *Mathematics of Computation, 62* (1994), 333-350.

[273] ———, "Finding a small root of a bivariate integer equation; factoring with high bits known", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070)*, 178-189, 1996.

[274] ——— "Finding a small root of a univariate modular equation", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070)*, 155-165, 1996.

[275] ———, "Analysis of ISO/CCITT Document X.509 Annex D", memorandum, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., June 11 1989.

[276] ———, "Two broken hash functions", IBM Research Report RC 18397, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Oct. 6 1992.

[277] D. COPPERSMITH, M. FRANKLIN, J. PATARIN, AND M. REITER, "Low-exponent RSA with related messages", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070)*, 1-9, 1996.

[278] D. COPPERSMITH, D.B. JOHNSON, AND S.M. MATYAS, "A proposed mode for triple-DES encryption", *IBM Journal of Research and Development, 40* (1996), 253-261.

[279] D. COPPERSMITH, H. KRAWCZYK, AND Y. MANSOUR, "The shrinking generator", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 22-39, 1994.

[280] D. COPPERSMITH, A.M. ODLZYKO, AND R. SCHROEPPEL, "Discrete logarithms in $GF(p)$", *Algorithmica,* 1 (1986), 1-15.

[281] D. COPPERSMITH AND P. ROGAWAY, "Software-efficient pseudorandom function and the use thereof for encryption", U.S. Patent # 5,454,039, 26 Sep 1995.

[282] T.H. CORMEN, C.E. LEISERSON, AND R.L. RIVEST, *Introduction to Algorithms,* MIT Press, Cambridge, Massachusetts, 1990.

[283] 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 (1992), 111-128.

[284] J.-M. COUVEIGNES, "Computing a square root for the number field sieve", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve,* volume 1554 of *Lecture Notes in Mathematics,* 95-102, Springer-Verlag, 1993.

[285] T. COVER AND R. KING, "A convergent gambling estimate of the entropy of English", *IEEE Transactions on Information Theory, 24* (1978), 413–421.

[286] R.E. CRANDALL, "Method and apparatus for public key exchange in a cryptographic system", U.S. Patent # 5,159,632, 27 Oct 1992.

[287] ———, "Method and apparatus for public key exchange in a cryptographic system", U.S. Patent # 5,271,061, 14 Dec 1993 (continuation-in-part of 5,159,632).

[288] R.A. CROFT AND S.P. HARRIS, "Public-key cryptography and re-usable shared secrets", H. Beker and F. Piper, editors, *Cryptography and Coding,* Institute of Mathematics & Its Applications (IMA), 189-201, Clarendon Press, 1989.

[339] Y. DESMEDT AND M. BURMESTER, "Towards practical 'proven secure' authenticated key distribution", *1st ACM Conference on Computer and Communications Security,* 228-23 1, ACM Press, 1993.

[340] Y. DESMEDT, C. GOUTIER, AND S. BENGIO, "Special uses and abuses of the Fiat-Shamir passport protocol", *Advances in Cryptology-CRYPTO '87 (LNCS 293),* 21–39, 1988.

[341] Y. DESMEDT AND A.M. ODLYZKO, "A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes", *Advances in Cryptology-CRYPTO '85 (LNCS 218), 516-522,* 1986.

[342] W. DIFFIE, '"The first ten years of public-key cryptography", *Proceedings of the IEEE, 76* (1988), 560-577.

[343] ———, "The first ten years of public key cryptology", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 135-175, IEEE Press, 1992. An earlier version appeared in [342].

[344] W. DIFFIE AND M.E. HELLMAN, "Multiuser cryptographic techniques", *Proceedings of AFIPS National Computer Conference,* 109-112, 1976.

[345] ———, "New directions in cryptography", *IEEE Transactions on Information Theory, 22* (1976), 644654.

[346] ——— "Exhaustive cryptanalysis of the NBS Data Encryption Standard", *Computer,* 10 (1977), 74-84.

[347] ———, "Privacy and authentication: An introduction to cryptography", *Proceedings of the IEEE, 67* (1979), 397427.

[348] W. DIFFIE, P.C. VAN OORSCHOT, AND M.J. WIENER, "Authentication and authenticated key exchanges", *Designs, Codes and Cryptography, 2* (1992), 107-l 25.

[349] C. DING, "The differential cryptanalysis and design of natural stream ciphers", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809),* 101–115, Springer-Verlag, 1994.

[350] B. DIXON AND A.K. LENSTRA, "Massively parallel elliptic curve factoring", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658),* 183–193, 1993.

[351] J.D. DIXON, "Asymptotically fast factorization of integers", *Mathematics of Computation, 36* (1981), 255-260.

[352] H. DOBBERTIN, "Cryptanalysis of MD4", *Journal of Cryptology,* to appear.

[353] ———, "RIPEMD with two-round compress function is not collision-free", *Journal of Cryptology,* to appear; announced at rump session, Eurocrypt '95.

[354] ———, "Cryptanalysis of MD4", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039), 53-69,* Springer-Verlag, 1996.

[355] H. DOBBERTIN, A. BOSSELAERS, AND B. PRENEEL, "RIPEMD-160: a strengthened version of RIPEMD", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039),* 71-82, Springer-Verlag, 1996.

[356] B. DODSON AND A.K. LENSTRA, "NFS with four large primes: An explosive experiment", *Advances in Cryptology-CRYPTO '95 (LNCS 963),* 372-385, 1995.

[357] D. DOLEV, C. DWORK, AND M. NAOR, "Non-malleable cryptography", *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 542-552,* 199 1.

[358] D. DOLEV AND A.C. YAO, "On the security of public key protocols", *Proceedings of the IEEE 22nd Annual Symposium on Foundations of Computer Science, 350-357,* 198 1.

[359] ———, "On the security of public key protocols", *IEEE Transactions on Information Theory,* 29 (1983), 198-208. An earlier version appeared in [358].

[360] P. DOWNEY, B. LEONG, AND R. SETHI, "Computing sequences with addition chains", *SIAM Journal on Computing,* 10 (1981), 638-646.

[361] S.R. DUSSÉ AND B.S. KALISKI JR., "A cryptographic library for the Motorola DSP 56000", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473), 230-244,* 1991.

[362] H. EBERLE, "A high-speed DES implementation for network applications", Advances in *Cryptology-CRYPTO '92 (LNCS 740),* 521–539, 1993.

[363] W. F. EHRSAM, C.H.W. MEYER, R.L. POWERS, J.L. SMITH, AND W.L. TUCHMAN, "Product block cipher system for data security", U.S. Patent # 3,962,539, 8 Jun 1976.

[313] W. DE JONGE AND D. CHAUM, "Attacks on some RSA signatures", *Advances in Cryptology-CRYPTO '85 (LNCS 218)*, 18-27, 1986.

[314] P. DE ROOIJ, "On the security of the Schnorr scheme using preprocessing", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547)*, 71–80, 1991.

[315] ——, "On Schnorr's preprocessing for digital signature schemes", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765)*, 435–439, 1994.

[316] ——, "Efficient exponentiation using precomputation and vector addition chains", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950), 389-399, 1995.*

[317] A. DE SANTIS, S. MICALI, AND G. PERSIANO, "Non-interactive zero-knowledge proof systems", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 52–72, 1988.

[318] A. DE SANTIS AND M. YUNG, "On the design of provably secure cryptographic hash functions", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473)*, 412–431, 1991.

[319] D. DE WALEFFE AND J.-J. QUISQUATER, "Better login protocols for computer networks", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741), 50-70,* Springer-Verlag, 1993.

[320] J.M. DELAURENTIS, "A further weakness in the common modulus protocol for the RSA cryptoalgorithm", *Cryptologia, 8* (1984), 253-259.

[321] N. DEMYTKO, "A new elliptic curve based analogue of RSA", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765)*, 40–49, 1994.

[322] B. DEN BOER, "Cryptanalysis of F.E.A.L.", *Advances in Cryptology-EUROCRYPT '88 (LNCS 330)*. 293–299, 1988.

[323] ——, "Diffie-Hellman is as strong as discrete log for certain primes", *Advances in Cryptology-CRYPTO '88 (LNCS 403)*, 530–539, 1990.

[324] B. DEN BOER AND A. BOSSELAERS, "An attack on the last two rounds of MD4", *Advances in Cryptology-CRYPTO '91 (LNCS 576)*, 194-203, 1992.

[325] —— ,"Collisions for the compression function of MD5", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765)*, 293–304, 1994.

[326] D.E. DENNING, *Cryptography and Data Security*, Addison-Wesley, Reading, Massachusetts, 1983. Reprinted with corrections.

[327] ——, "Digital signatures with RSA and other public-key cryptosystems", *Communications of the ACM, 27* (1984), *388-392.*

[328] ——, 'To tap or not to tap", *Communications of the ACM, 36* (1993), 24–44.

[329] D.E. DENNING AND D.K. BRANSTAD, "A taxonomy for key escrow encryption systems", *Communications of the ACM, 39* (1996), 34-40.

[330] D.E. DENNING AND G.M. SACCO, "Timestamps in key distribution protocols", *Communications of the ACM, 24* (1981), 533-536.

[331] D.E. DENNING AND M. SMID, "Key escrowing today", *IEEE Communications Magazine,* 32 (September 1994), 58-68.

[332] J. B. DENNIS AND E. C. VAN HORN, "Programming semantics for multiprogrammed computations", *Communications of the ACM,* 9 (1966), 143-155.

[333] T. DENNY, B. DODSON, A.K. LENSTRA, AND M.S. MANASSE, "On the factorization of RSA-120", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 166-174, 1994.

[334] DEPARTMENTOF DEFENSE (U.S.), "Department of defense password management guideline", CSC-STD-002-85, Department of Defense Computer Security Center, Fort Meade, Maryland, 1985.

[335] Y. DESMEDT, "Unconditionally secure authentication schemes and practical and theoretical consequences", *Advances in Cryptology-CRYPTO '85 (LNCS 218), 42-*55, 1986.

[336] ——, "Society and group oriented cryptography: A new concept", *Advances in Cryptology-CRYPTO '87 (LNCS 293)*, 120–127, 1988.

[337] ——, '"Threshold cryptography", *European Transactions on Telecommunications, 5* (1994), 449–457.

[338] ——, "Securing traceability of ciphertexts – Towards a secure software key escrow system", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921)*, 147-157, 1995.

[390] P. FELDMAN, "A practical scheme for non-interactive verifiable secret sharing", *Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science*, 427-437, 1987.

[391] D.C. FELDMEIER AND P.R. KARN, "UNIX password security-ten years later", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 44-63, 1990.

[392] W. FELLER, *An Introduction to Probability Theory and its Applications*, John Wiley & Sons, New York, 3rd edition, 1968.

[393] A. FIAT AND M. NAOR, "Rigorous time/space tradeoffs for inverting functions", *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, 534-541, 1991.

[394] ——— "Broadcast encryption", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 480-491, 1994.

[395] A. FIAT AND A. SHAMIR, "How to prove yourself: Practical solutions to identification and signature problems", *Advances in Cryptology-CRYPTO '86 (LNCS 263)*, 186–194, 1987.

[396] FIPS 46, "Data encryption standard", Federal Information Processing Standards Publication 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977 (revised as FIPS 46-l: 1988; FIPS 46-2: 1993).

[397] FIPS 74, "Guidelines for implementing and using the NBS data encryption standard", Federal Information Processing Standards Publication 74, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1981.

[398] FIPS 8 1, "DES modes of operation", Federal Information Processing Standards Publication 8 1, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1980.

[399] FIPS 112, "Password usage", Federal Information Processing Standards Publication 112, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1985.

[400] FIPS 113, "Computer data authentication", Federal Information Processing Standards Publication 113, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1985.

[401] FIPS 140- 1, "Security requirements for cryptographic modules", Federal Information Processing Standards Publication 140-1, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.

[402] FIPS 171, "Key management using ANSI X9.17", Federal Information Processing Standards Publication 171, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1992.

[403] FIPS 180, "Secure hash standard", Federal Information Processing Standards Publication 180, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, May 11 1993.

[404] FIPS 180- 1, "Secure hash standard", Federal Information Processing Standards Publication 180-1, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, April 17 1995 (supersedes FIPS PUB 180).

[405] FIPS 185, "Escrowed encryption standard (EES)“, Federal Information Processing Standards Publication 185, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.

[406] FIPS 186, "Digital signature standard", Federal Information Processing Standards Publication 186, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.

[407] FIPS JJJ, "Standard for public key cryptographic entity authentication mechanisms", U.S. Department of Commerce/N.I.S.T., draft (1996 March 29).

[408] A.M. FISCHER, "Public key/signature cryptosystem with enhanced digital signature certification", U.S. Patent # 4,868,877, 19 Sep 1989.

[409] ———, "Public key/signature cryptosystem with enhanced digital signature certification", U.S. Patent # 5,005,200, 2 Apr 1991 (continuation-in-part of 4,868,877).

[410] ———, "Electronic document authorization", *Proceedings of the 13th National Computer*

[364] W.F. EHRSAM, S.M. MATYAS, C.H. MEYER, AND W.L. TUCHMAN, "A cryptographic key management scheme for implementing the Data Encryption Standard", *IBM Systems Journal,* 17 (1978), 106-125.

[365] ELECTRONIC INDUSTRIES ASSOCIATION (EIA), "Dual-mode mobile station – base station compatibility standard", EIA Interim Standard IS-54 Revision B (Rev. B), 1992.

[366] T. ELGAMAL, *Cryptography and logarithms over finite fields,* PhD thesis, Stanford University, 1984.

[367] ———, "A public key cryptosystem and a signature scheme based on discrete logarithms", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196),* 10–18, 1985.

[368] ———, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory,* 31 (1985), 469-472. An earlier version appeared in [367].

[369] ———, "A subexponential-time algorithm for computing discrete logarithms over GF(p^2)", *IEEE Transactions on Information Theory,* 31 (1985), 473–481.

[370] P. ELIAS, 'The efficient construction of an unbiased random sequence", *The Annals of Mathematical Statistics, 43* (1972), 865-870.

[371] ———, "Interval and recency rank source encoding: Two on-line adaptive variable-length schemes", *IEEE Transactions on Information Theory, 33* (1987), 3-10.

[372] E.D. ERDMANN, "Empirical tests of binary keystreams", Master's thesis, Department of Mathematics, Royal Holloway and Bedford New College, University of London, 1992.

[373] P. ERDÖS AND C. POMERANCE, "On the number of false witnesses for a composite number", *Mathematics of Computation, 46* (1986), 259-279.

[374] D. ESTES, L.M. ADLEMAN, K. KOMPELLA, K.S. MCCURLEY, AND G.L. MILLER, "Breaking the Ong-Schnorr-Shamir signature scheme for quadratic number fields", *Advances in Cryptology-CRYPTO '85 (LNCS 218),* 3-13, 1986.

[375] A. EVANS JR., W. KANTROWITZ, AND E. WEISS, "A user authentication scheme not requiring secrecy in the computer", *Communications of the ACM,* 17 (1974), 437-442.

[376] S. EVEN AND 0. GOLDREICH, "On the power of cascade ciphers", *ACM Transactions on Computer Systems, 3* (1985), 108-l 16.

[377] S. EVEN, 0. GOLDREICH, AND S. MICALI, "On-line/off-line digital signatures", *Advances in Cryptology-CRYPTO '89 (LNCS 435),* 263-275, 1990.

[378] ———, "On-line/off-line digital signatures", *Journal of Cryptology, 9* (1996), 35-67. An earlier version appeared in [377].

[379] S. EVEN AND Y. YACOBI, "Cryptocomplexity and NP-completeness", J.W. de Bakker and J. van Leeuwen, editors, *Automata, Languages, and Programming, 7th Colloquium (LNCS 85),* 195-207, Springer-Verlag, 1980.

[380] D. EVERETT, "Identity verification and biometrics", K.M. Jackson and J. Hruska, editors, *Computer Security Reference Book, 37-*73, CRC Press, 1992.

[381] J.-H. EVERTSE AND E. VAN HEYST, "Which new RSA-signatures can be computed from certain given RSA-signatures?", *Journal of Cryptology, 5* (1992), 41-52.

[382] R.C. FAIRFIELD, R.L. MORTENSON, AND K.B. COULTHART, "An LSI random number generator (RNG)", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196),* 203–230, 1985.

[383] U. FEIGE, A. FIAT, AND A. SHAMIR, "Zero-knowledge proofs of identity", *Journal of Cryptology,* 1 (1988), 77-94.

[384] U. FEIGE AND A. SHAMIR, "Witness indistinguishable and witness hiding protocols", *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing,* 416-426, 1990.

[385] H. FEISTEL, "Block cipher cryptographic system", U.S. Patent # 3,798,359, 19 Mar 1974.

[386] ———, "Step code ciphering system", U.S. Patent # 3,798,360, 19 Mar 1974.

[387] ———, "Cryptography and computer privacy", *Scientific American, 228* (May 1973), 15-23.

[388] H. FEISTEL, W.A. NOTZ, AND J.L. SMITH, "Some cryptographic techniques for machine-to-machine data communications", *Proceedings of the IEEE, 63* (1975), 1545-l 554.

[389] F.A. FELDMAN, "Fast spectral tests for measuring nonrandomness and the DES", *Advances in Cryptology-CRYPTO '87 (LNCS 293),* 243-254, 1988.

I4341 E.M. GABIDULIN, "On public-key cryptosystems based on linear codes: Efficiency and weakness", P.G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, 17-31, Institute of Mathematics & Its Applications (IMA), 1995.

[435] E.M. GABIDULIN, A.V. PARAMONOV, AND O.V. TRETJAKOV, "Ideals over a non-commutative ring and their application in cryptology", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547), 482489,* 1991.

[436] H. GAINES, *Cryptanalysis: A Study **of** Ciphers and their Solutions,* Dover Publications, New York, 1956.

[437] J. GAIT, "A new nonlinear pseudorandom number generator", *IEEE Transactions on Software Engineering, 3* (1977), 359-363.

[438] J.M. GALVIN, K. MCCLOGHRIE, AND J.R. DAVIN, "Secure management of SNMP networks", *Integrated Network Management, II,* 703-714, 1991.

[439] R.A. GAMES AND A.H. CHAN, "A fast algorithm for determining the complexity of a binary sequence with period 2^n", *IEEE Transactions on Information Theory, 29* (1983), 144-146.

[440] M. GARDNER, "A new kind of cipher that would take millions of years to break", *Scientific American, 237* (Aug 1977), 120-124.

[441] M.R. GAREY AND D.S. JOHNSON, *Computers and Intractability: A Guide to the Theory **of** NP-completeness,* W.H. Freeman, San Francisco, 1979.

I4421 S. GARFINKEL, *PGP: Pretty Good Privacy,* O'Reilly and Associates, Inc., Sebastopol, California, 1995.

[443] H. GARNER, "The residue number system", *IRE Transactions on Electronic Computers,* EC-8 (1959), 140-147.

[444] C.F. GAUSS, *Disquisitiones **Arithmeticae**,* 1801. English translation by Arthur A. Clarke, Springer-Verlag, New York, 1986.

[445] K. GEDDES, S. CZAPOR, AND G. LABAHN, *Algorithms **for** Computer Algebra,* Kluwer Academic Publishers, Boston, 1992.

[446] P. GEFFE, "How to protect data with ciphers that are really hard to break", *Electronics, 46* (1973), 99-101.

[447] J. GEORGIADES, "Some remarks on the security of the identification scheme based on permuted kernels", *Journal **of** Cryptology, 5* (1992), 133-137.

[448] J. GERVER, "Factoring large numbers with a quadratic sieve", *Mathematics **of** Computation,* 41 (1983), 287-294.

[449] P.J. GIBLIN, *Primes and Programming: An Introduction to Number Theory with Computing,* Cambridge University Press, Cambrige, 1993.

[450] J.K. GIBSON, "Some comments on Damgård's hashing principle", *Electronics Letters,* 26 (July 19, 1990), 1178-1179.

[451] ——, "Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547),* 517-521, 1991.

[452] ——, "Severely denting the Gabidulin version of the McEliece public key cryptosystem", *Designs, Codes and Cryptography, 6* (1995), 37–45.

[453] ——, 'The security of the Gabidulin public key cryptosystem", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070),* 212-223, 1996.

[454] E.N. GILBERT, F.J. MACWILLIAMS, AND N.J.A. SLOANE, "Codes which detect deception", *Bell System Technical Journal, 53* (1974), 405–424.

[455] H. GILBERT AND G. CHASSÉ, "A statistical attack of the Feal-8 cryptosystem", *Advances in Cryptology-CRYPTO '90 (LNCS 537),* 22-33, 1991.

[456] H. GILBERT AND P. CHAUVAUD, "A chosen plaintext attack of the 16-round Khufu cryptosystem", *Advances in Cryptology-CRYPTO '94 (LNCS 839), 359-368,* 1994.

[457] M. GIRAULT, "Hash-functions using modulo-n operations", *Advances in Cryptology-EUROCRYPT '87 (LNCS 304),* 217-226, 1988.

[458] ——, "An identity-based identification scheme based on discrete logarithms modulo a composite number", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473),* 481–486, 1991.

[459] ——, "Self-certified public keys", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547),* 490–497, 1991.

Security Conference, Washington D. C., sponsored by N.I.S.T. and the National Computer Security Center, USA, 1990.

[411] J.-B. Fischer and J. Stern, “‘An efficient pseudo-random generator provably as secure as syndrome decoding”, *Advances in Cryptology-EUROCRYPT ‘96 (LNCS 1070)*, 245–255, 1996.

[412] M. Fischer, S. Micali, and C. Rackoff, “A secure protocol for oblivious transfer”, unpublished (presented at Eurocrypt’84).

[413] P. Flajolet and A. Odlyzko, “Random mapping statistics”, *Advances in Cryptology-EUROCRYPT ‘89 (LNCS 434), 329-354,* 1990.

[4141 W. Ford, *Computer Communications Security: Principles, Standard Protocols and Techniques,* Prentice Hall, Englewood Cliffs, New Jersey, 1994.

[415] ———, “Standardizing information technology security”, *StandardView, 2* (1994), 64–71.

[416] ———, “Advances in public-key certificate standards”, *Security, Audit and Control,* 13 (1995), ACM Press/SIGSAC, 9-15.

[417] W. Ford and M. Wiener, “A key distribution method for object-based protection”, *2nd ACM Conference on Computer and Communications Security,* 193-197, ACM Press, 1994.

[418] R. Forré, “A fast correlation attack on nonlinearly feedforward filtered shift-register sequences”, *Advances in Cryptology-EUROCRYPT ‘89 (LNCS 434), 586-595,* 1990.

[419] Y. Frankel and M. Yung, “Cryptanalysis of the immunized LL public key systems”, *Advances in Cryptology-CRYPTO ‘95 (LNCS 963)*, 287-296, 1995.

[420] ———, “Escrow encryption systems visited: Attacks, analysis and designs”, *Advances in Cryptology-CRYPTO ‘95 (LNCS 963), 222-*235, 1995.

[421] M.K. Franklin and M.K. Reiter, “Verifiable signature sharing”, *Advances in Cryptology-EUROCRYPT ‘95 (LNCS 921)*, 50–63, 1995.

[422] G. Frey and H.-G. Rück, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”, *Mathematics of Computation, 62* (1994), 865–874.

[423] W. Friedman, *Military Cryptanalysis,* U.S. Government Printing Office, Washington DC, 1944. Volume I – Monoalphabetic substitution systems. Volume II – Simpler varieties of polyalphabetic substitution systems. Volume III – Aperiodic substitutions. Volume IV -Transposition systems.

[424] ———, “Cryptology”, *Encyclopedia Brittanica, 6* (1967), 844–85 1.

[425] ——— *Elements of Cryptanalysis,* Aegean Park Press, Laguna Hills, California, 1976. First published in 1923.

[426] ———, *The Index of Coincidence and its Applications in Cryptography,* Aegean Park Press, Laguna Hills, California, 1979. First published in 1920.

[427] A.M. Frieze, J. Håstad, R. Kannan, J.C. Lagarias, and A. Shamir, “Reconstructing truncated integer variables satisfying linear congruences”, *SIAM Journal on Computing,* 17 (1988), 262-280.

[428] A. Fuiioka, T. Okamoto, and S. Miyaguchi, “ESIGN: An efficient digital signature implementation for smart cards”, *Advances in Cryptology-EUROCRYPT ‘91 (LNCS 547)*, 446–457, 1991.

[429] W. Fumy and P. Landrock, “Principles of key management”, *IEEE Journal on Selected Areas in Communications,* 11 (1993), 785–793.

[430] W. Fumy and M. Leclerc, “Placement of cryptographic key distribution within OSI: design alternatives and assessment”, *Computer Networks and ISDN Systems, 26* (1993), 217-225.

[431] W. Fumy and M. Munzert, “A modular approach to key distribution”, *Advances in Cryptology-CRYPTO ‘90 (LNCS 537), 274-*283, 1991.

[432] W. Fumy and M. Rietenspiess, “Open systems security standards”, Encyclopedia of Computer Science and Technology, A. Kent, J.G. Williams, C.M. Hall, eds., Marcel Dekker, New York (to appear, 1996).

[433] K. Gaarder and E. Snekkenes, “Applying a formal analysis technique to the CCITT X.509 strong two-way authentication protocol”, *Journal of Cryptology, 3* (1991), 81-98.

[482] S. GOLDWASSER, S. MICALI, AND R.L. RIVEST, "A "paradoxical" solution to the signature problem", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science*, 441–448, 1984.

[483] ——, "A "Paradoxical" solution to the signature problem", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196)*, 467, 1985.

[484] ——, "A digital signature scheme secure against adaptive chosen-message attacks", *SIAM Journal on Computing*, 17 (1988), 281–308. Earlier versions appeared in [482] and [483].

[485] J. GOLIĆ, "Correlation via linear sequential circuit approximation of combiners with memory", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658)*, 113-123, 1993.

[486] ——, "On the security of shift register based keystream generators", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 90-100, Springer-Verlag, 1994.

[487] ——, "Intrinsic statistical weakness of keystream generators", *Advances in Cryptology-ASIACRYPT '94 (LNCS 917)*, 91-103, 1995.

[488] —— "Linear cryptanalysis of stream ciphers": B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 154-169, Springer-Verlag, 1995.

[489] ——, "Towards fast correlation attacks on irregularly clocked shift registers", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921)*, 248-262, 1995.

[490] —— "On the security of nonlinear filter generators", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 173-188, Springer-Verlag, 1996.

[491] J. GOLIĆ AND M. MIHALJEVIĆ, "A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance", *Journal of Cryptology, 3* (1991), 201-212.

[492] J. GOLIĆ AND L. O'CONNOR, 'Embedding and probabilistic correlation attacks on clock-controlled shift registers", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950)*, 230–243, 1995.

[493] R.A. GOLLIVER, A.K. LENSTRA, AND K.S. MCCURLEY, "Lattice sieving and trial division", *Algorithmic Number Theory (LNCS 877)*, 18-27, 1994.

[494] D. GOLLMANN, "Pseudo random properties of cascade connections of clock controlled shift registers", *Advances in Cryptology-Proceedings of EUROCRYPT84 (LNCS 209)*, 93–98, 1985.

[495] ——, "Cryptanalysis of clock controlled shift registers", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 121-126, Springer-Verlag, 1994.

[496] D. GOLLMANN AND W.G. CHAMBERS, "Clock-controlled shift registers: a review", *IEEE Journal on Selected Areas in Communications, 7* (1989), 525-533.

[497] D. GOLLMANN, Y. HAN, AND C. MITCHELL, "Redundant integer representations and fast exponentiation", *Designs, Codes and Cryptography*, 7 (1996), 135-151.

[498] S.W. GOLOMB, *Shift Register Sequences*, Holden-Day, San Francisco, 1967. Reprinted by Aegean Park Press, 1982.

[499] L. GONG, "Using one-way functions for authentication", *Computer Communication Review*, 19 (1989), 8-11.

[500] ——, "A security risk of depending on synchronized clocks", *Operating Systems Review, 26* (1992), 49-53.

[501] ——, "Variations on the themes of message freshness and replay", *The Computer Security* Foundations *Workshop VI*, 131-136, IEEE Computer Society Press, 1993.

[502] ——, "New protocols for third-party-based authentication and secure broadcast", *2nd ACM Conference on Computer and Communications Security*, 176-l 83, ACM Press, 1994.

[503] ——, "Efficient network authentication protocols: lower bounds and optimal implementations", *Distributed Computing, 9* (1995), 131-145.

[504] L. GONG, T.M.A. LOMAS, R.M. NEEDHAM, AND J.H. SALTZER, "Protecting poorly chosen secrets from guessing attacks", *IEEE Journal on Selected Areas in Communications*, 11 (1993), 648-656.

[460] M. GIRAULT, R. COHEN, AND M. CAMPANA, "A generalized birthday attack", *Advances in Cryptology-EUROCRYPT '88 (LNCS 330)*, 129-156, 1988.

[461] M. GIRAULT AND J.C. PAILLÈS, "An identity-based scheme providing zero-knowledge authentication and authenticated key-exchange", *First European Symposium on Research in Computer Security – ESORICS'90*, 173–184, 1990.

[462] M. GIRAULT AND J. STERN, "On the length of cryptographic hash-values used in identification schemes", *Advances in Cryptology-CRYPTO '94 (LNCS 839)*, 202–215, 1994.

[463] V.D. GLIGOR, R. KAILAR, S. STUBBLEBINE, AND L. GONG, "Logics for cryptographic protocols — virtues and limitations", *The Computer Security Foundations Workshop IV*, 219-226, IEEE Computer Security Press, 1991.

[464] C.M. GOLDIE AND R.G.E. PINCH, *Communication Theory*, Cambridge University Press, Cambridge, 1991.

[465] 0. GOLDREICH, 'Two remarks concerning the Goldwasser-Micali-Rivest signature scheme", *Advances in Cryptology-CRYPTO '86 (LNCS 263)*, 104-110, 1987.

[466] 0. GOLDREICH, S. GOLDWASSER, AND S. MICALI, "How to construct random functions", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, 464-479,* 1984.

[467] ——, "On the cryptographic applications of random functions", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196)*, 276-288, 1985.

[468] ——, "How to construct random functions", *Journal of the Association for Computing Machinery, 33* (1986), 792-807. An earlier version appeared in [466].

[469] 0. GOLDREICH AND H. KRAWCZYK, "On the composition of zero-knowledge proof systems", MS. Paterson, editor, *Automata, Languages and Programming, 17th International Colloquium (LNCS 443)*, 268-282, Springer-Verlag, 1990.

[470] 0. GOLDREICH, H. KRAWCZYK, AND M. LUBY, "On the existence of pseudorandom generators", *Proceedings of the IEEE 29th Annual Symposium on Foundations of Comvuter Science.* 12-24. 1988.

[471] 0. GOLDREICH AND L.A. LEVIN, "A hard-core predicate for all one-way functions", *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, 25-32,* 1989.

[472] 0. GOLDREICH, S. MICALI, AND A. WIGDERSON, "Proofs that yield nothing but their validity and a methodology of cryptographic protocol design", *Proceedings of the IEEE 27th Annual Symposium on Foundations of Computer Science,* 174-187, 1986.

[473] —— "How to prove all NP statements in zero-knowledge, and a methodology of cryptographic protocol design", *Advances in Cryptology-CRYPTO '86 (LNCS 263)*, 171-185, 1987.

[474] ——, "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* (1991), 691-729. An earlier version appeared in [472].

[475] 0. GOLDREICH AND Y. OREN, "Definitions and properties of zero-knowledge proof systems", *Journal of Cryptology, 7* (1994), l-32.

[476] S. GOLDWASSER, "The search for provably secure cryptosystems", C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume *42* of *Proceedings of Symposia in Applied Mathematics,* 89-l 13, American Mathematical Society, 1990.

[477] S. GOLDWASSER AND J. KILIAN, "Almost all primes can be quickly certified", *Proceedings of the 18th Annual ACM Symposium on Theory of Computing,* 316-329, 1986.

[478] S. GOLDWASSER AND S. MICALI, "Probabilistic encryption &how to play mental poker keeping secret all partial information", *Proceedings of the 14th Annual ACM Symposium on Theory of Computing, 365-377,* 1982.

[479] —— "Probabilistic encryption", *Journal of Computer and System Sciences, 28* (1984), *270-299.* An earlier version appeared in [478].

[480] S. GOLDWASSER, S. MICALI, AND C. RACKOFF, "The knowledge complexity of interactive proof-systems", *Proceedings of the 17th Annual ACM Symposium on Theory of Computing,* 291-304, 1985.

[481] ——, "The knowledge complexity of interactive proof systems", *SIAM Journal on Computing,* 18 (1989), 186-208. An earlier version appeared in [480].

EUROCRYPT '88 (LNCS 330), 405–414, 1988.

[530] ———, "An identity-based key-exchange protocol", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434), 29-37,* 1990.

[531] H. GUSTAFSON, *Statistical Analysis **of** Symmetric Ciphers,* PhD thesis, Queensland University of Technology, 1996.

[532] H. GUSTAFSON, E. DAWSON, AND J. GOLIĆ, "Randomness measures related to subset occurrence", E. Dawson and J. Golić, editors, *Cryptography: Policy and Algorithms, International Conference, Brisbane, Queensland, Australia, July 1995 (LNCS 1029),* 132-143, 1996.

[533] H. GUSTAFSON, E. DAWSON, L. NIELSEN, AND W. CAELLI, "A computer package for measuring the strength of encryption algorithms", *Computers & Security,* 13 (1994), 687-697.

[534] A. GUYOT, "OCAPI: Architecture of a VLSI coprocessor for the gcd and extended gcd of large numbers", *Proceedings **of** the 10th IEEE Symposium on Computer Arithmetic,* 226–23 1, IEEE Press, 1991.

[535] S. HABER AND W.S. STORNETTA, "How to time-stamp a digital document", *Journal **of** Cryptology, 3* (199 1), 99-111.

[536] J.L. HAFNER AND K.S. MCCURLEY, "On the distribution of running times of certain integer factoring algorithms", *Journal **of** Algorithms,* 10 (1989), 531-556.

[537] ———, "A rigorous subexponential algorithm for computation of class groups", *Journal **of** the American Mathematical Society, 2* (1989), 837-850.

[538] T. HANSEN AND G.L. MULLEN, "Primitive polynomials over finite fields", *Mathematics **of** Computation, 59* (1992), 639-643.

[539] G.H. HARDY, *A Mathematician5 Apology,* Cambridge University Press, London, 1967.

[540] G.H. HARDY AND E.M. WRIGHT, ***An Introduction** to the Theory **of** Numbers,* Clarendon Press, Oxford, 5th edition, 1979.

[541] C. HARPES, G.G. KRAMER, AND J.L. MASSEY, "A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921), 24-38, 1995.*

[542] V. HARRIS, "An algorithm for finding the greatest common divisor", *Fibonacci Quarterly, 8* (1970), 102-103.

[543] J. H.&TAD, A.W. SCHRIFT, AND A. SHAMIR, "The discrete logarithm modulo a composite hides O(n) bits", *Journal **of** Computerand System Sciences, 47* (1993), 376-404.

[544] J. HÅSTAD, "Solving simultaneous modular equations of low degree", *SIAM Journal on Computing, 17* (1988), 336-341.

[545] ———, "Pseudo-random generators under uniform assumptions", *Proceedings **of the** 22nd Annual ACM Symposium on Theory **of** Computing, 395-404,* 1990.

[546] R. HEIMAN, "A note on discrete logarithms with special structure", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658),* 454–457, 1993.

[547] ——— "Secure audio teleconferencing: A practical solution", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658),* 437–448, 1993.

[548] M.E. HELLMAN, "An extension of the Shannon theory approach to cryptography", *IEEE Transactions on Information Theory, 23* (1977), 289-294.

[549] ———, "A cryptanalytic time-memory tradeoff", *IEEE Transactions on Information Theory,* 26 (1980), 401-406.

[550] M.E. HELLMAN AND C.E. BACH, "Method and apparatus for use in public-key data encryption system", U.S. Patent # 4,633,036, 30 Dec 1986.

[551] M.E. HELLMAN, B.W. DIFFIE, AND R.C. MERKLE, "Cryptographic apparatus and method", U.S. Patent # 4,200,770, 29 Apr 1980.

[552] M.E. HELLMAN, R. MERKLE, R. SCHROEPPEL, L. WASHINGTON, W. DIFFIE, S. POHLIG, AND P. SCHWEITZER, "Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard", Technical Report SEL 76-042, Information Systems Laboratory, Stanford University, Palo Alto, California, Sept. 9 1976 (revised Nov 10 1976).

[553] M.E. HELLMAN AND R.C. MERKLE, "Public key cryptographic apparatus and method", U.S. Patent # 4,218,582, 19 Aug 1980.

[554] M.E. HELLMAN AND S.C. POHLIG, "Exponentiation cryptographic apparatus and method", U.S. Patent # 4,424,414, 3 Jan 1984.

[505] L. Gong, R. Needham, and R. Yahalom, “Reasoning about belief in cryptographic protocols”, *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 234-248,* 1990.

[506] L. Gong and D.J. Wheeler, “A matrix key-distribution scheme”, *Journal of Cryptology,* 2 (1990), 5 1-59.

[507] I.J. Good, ‘The serial test for sampling numbers and other tests for randomness”, *Proceedings of the Cambridge Philosophical Society, 49* (1953), 276-284.

[508] ——–, “On the serial test for random sequences”, *The Annals of Mathematical Statistics, 28* (1957), 262-264.

[509] D.M. Gordon, “Designing and detecting trapdoors for discrete log cryptosystems”, *Advances in Cryptology-CRYPTO ‘92 (LNCS 740),* 66-75, 1993.

[510] ——–, “Discrete logarithms in GF(P) using the number field sieve”, *SIAM Journal on Discrete Mathematics, 6* (1993), 124-138.

[511] D.M. Gordon and K.S. McCurley, “Massively parallel computations of discrete logarithms”, *Advances in Cryptology-CRYPTO ‘92 (LNCS 740), 3 12-323, 1993.*

[512] J. Gordon, “Very simple method to find the minimum polynomial of an arbitrary nonzero element of a finite field”, *Electronics Letters,* 12 (December 9, 1976), 663-664.

[513] ——–, “Strong RSA keys”, *Electronics Letters,* 20 (June 7, 1984), 514-516.

[514] ——– “Strong primes are easy to find”, *Advance; in Cryptology-Proceedings of EUROCRYPT84 (LNCS 209),* 216-223, 1985.

[515] ——– “How to forge RSA key certificates”, *Electronics Letters,* 21 (April 25, 1985), 377-379.

[516] ——– “Fast multiplicative inverse in modular arithmetic”, H. Beker and F. Piper, editors, *Cryptography and Coding,* Institute of Mathematics & Its Applications (IMA), 269-279, Clarendon Press, 1989.

[517] J. Gordon and H. Retkin, “Are big *S*-boxes best?‘, *Cryptography-Proceedings of the Workshop on Cryptography, Burg Feuerstein (LNCS 149), 257-262,* 1983.

[518] M. Goresky and A. Klapper, “Feedback registers based on ramified extensions of the 2-adic numbers”, *Advances in Cryptology-EUROCRYPT ‘94 (LNCS 950), 215-222,* 1995.

[519] K.C. Goss, “Cryptographic method and apparatus for public key exchange with authentication”, U.S. Patent # 4,956,863, 11 Sep 1990.

[520] R. Graham, D. Knuth, and 0. Patashnik, *Concrete Mathematics,* Addison-Wesley, Reading, Massachusetts, 2nd edition, 1994.

[521] A. Granville, “Primality testing and Carmichael numbers”, *Notices of the American Mathematical Society, 39* (1992), 696-700.

[522] E. Grossman, “Group theoretic remarks on cryptographic systems based on two types of addition”, IBM Research Report RC 4742, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Feb. 26 1974.

[523] L.C. Guillou and J.-J. Quisquater, “Method and apparatus for authenticating accreditations and for authenticating and signing messages”, U.S. Patent # 5,140,634, 18 Aug 1992.

[524] ——–, “A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory”, *Advances in Cryptology-EUROCRYPT ‘88 (LNCS 330),* 123-128, 1988.

[525] L.C. Gljillou, J.-J. Quisquater, M. Walker, P. Landrock, and C. Shaer, “Precautions taken against various potential attacks in ISO/IEC DIS 9796”, *Advances in Cryptology-EUROCRYPT ‘90 (LNCS 473),* 465–473, 1991.

[526] L.C. Guillou and M. Ugon, “Smart card – a highly reliable and portable security device”, *Advances in Cryptology-CRYPTO ‘86 (LNCS 263), 464-479,* 1987.

[527] L.C. Guillou, M. Ugon, and J.-J. Quisquater, ‘The smart card: A standardized security device dedicated to public cryptology”, G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 561-613, IEEE Press, 1992.

[528] C.G. Gunther, “Alternating step generators controlled by de Bruijn sequences”, *Advances in Cryptology-EUROCRYPT ‘87 (LNCS 304),* 5-14, 1988.

[529] ——–, “A universal algorithm for homophonic coding”, *Advances in Cryptology-*

[579] IS0 9564-1, "Banking – Personal Identification Number management and security – Part 1: PIN protection principles and techniques", International Organization for Standardization, Geneva, Switzerland, 1990.

[580] IS0 9564-2, "Banking -Personal Identification Number management and security – Part 2: Approved algorithm(s) for PIN encipherment", International Organization for Standardization, Geneva, Switzerland, 1991.

[581] IS0 9807, "Banking and related financial services – Requirements for message authentication (retail)“, International Organization for Standardization, Geneva, Switzerland, 1991.

[582] IS0 10126- 1, "Banking – Procedures for message encipherment (wholesale) – Part 1: General principles", International Organization for Standardization, Geneva, Switzerland, 1991.

[583] ISO 10126-2, "Banking – Procedures for message encipherment (wholesale) – Part 2: Algorithms", International Organization for Standardization, Geneva, Switzerland, 1991.

[584] IS0 10202-7, "Financial transaction cards – Security architecture of financial transaction systems using integrated circuit cards -Part 7: Key management", draft (DIS), 1994.

[585] IS0 1113 1, "Banking – Financial institution sign-on authentication", International Organization for Standardization, Geneva, Switzerland, 1992.

[586] ISO 11166- 1, "Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats", International Organization for Standardization, Geneva, Switzerland, 1994.

[587] IS0 11166-2, "Banking – Key management by means of asymmetric algorithms – Part 2: Approved algorithms using the RSA cryptosystem", International Organization for Standardization, Geneva, Switzerland, 1995.

[588] IS0 11568-1, "Banking- Key management (retail) – Part 1: Introduction to key management", International Organization for Standardization, Geneva, Switzerland, 1994.

[589] ISO 11568-2, "Banking – Key management (retail) – Part 2: Key management techniques for symmetric ciphers", International Organization for Standardization, Geneva, Switzerland, 1994.

[590] IS0 11568-3, "Banking – Key management (retail) – Part 3: Key life cycle for symmetric ciphers", International Organization for Standardization, Geneva, Switzerland, 1994.

[591] IS0 11568-4, "Banking – Key management (retail) – Part 4: Key management techniques using public key cryptography", draft (DIS), 1996.

[592] ISO 11568-5, "Banking – Key management (retail) – Part 5: Key life cycle for public key cryptosystems", draft (DIS), 1996.

[593] ISO 11568-6, "Banking – Key management (retail) – Part 6: Key management schemes", draft (CD), 1996.

[594] ISO/IEC 9594- 1, "Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models, and services", International Organization for Standardization, Geneva, Switzerland, 1995 (equivalent to ITU-T Rec. X.500, 1993).

[595] ISO/IEC 9594-8, "Information technology – Open Systems Interconnection – The Directory: Authentication framework", International Organization for Standardization, Geneva, Switzerland, 1995 (equivalent to ITU-T Rec. X.509, 1993).

[596] ISO/IEC 9796, "Information technology – Security techniques – Digital signature scheme giving message recovery", International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).

[597] ISO/IEC 9797, "Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1994 (second edition).

[598] ISO/IEC 9798- 1, "Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model", International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).

[599] ISO/IEC 9798-2, "Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms", International Organization for Standardization, Geneva, Switzerland, 1994 (first edition).

[600] ISO/IEC 9798-3, "Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authen-

[555] M.E. HELLMAN AND J.M. REYNERI, "Fast computation of discrete logarithms in GF(q)", *Advances in Cryptology–Proceedings of Crypto 82,* 3-l 3, 1983.

[556] I.N. HERSTEIN, *Topics in Algebra,* Xerox College Pub., Lexington, Massachusetts, 2nd edition, 1975.

[557] L.S. HILL, "Cryptography in an algebraic alphabet", *American Mathematical Monthly, 36* (1929), 306-312.

[558] L.J. HOFFMAN, *Modem Methods for Computer Security and Privacy,* Prentice Hall, Englewood Cliffs, New Jersey, 1977.

[559] R.V. HOGG AND E.A. TANIS, *Probability and statistical inference,* Macmillan Publishing Company, New York, 3rd edition, 1988.

[560] W. HOHL, X. LAI, T. MEIER, AND C. WALDVOGEL, "Security of iterated hash functions based on block ciphers", *Advances in Cryptology-CRYPTO '93 (LNCS 773),* 379–390, 1994.

[561] S.-M. HONG, S.-Y. OH, AND H. YOON, "New modular multiplication algorithms for fast modular exponentiation", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070),* 166–177, 1996.

[562] P. HORSTER AND H.-J. KNOBLOCH, "Discrete logarithm based protocols", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547),* 399–408, 1991.

[563] P. HORSTER, M. MICHELS, AND H. PETERSEN, "Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications", *Advances in Cryptology-ASIACRYPT* '94 *(LNCS 917), 224-237, 1995.*

[564] P. HORSTER AND H. PETERSEN, "Generalized ElGamal signatures (in German)", *Sicherheit in Informationssystemen, Proceedings der Fachtagung SIS'94*, 89-106, Verlag der Fachvereine Zurich, 1994.

[565] T.W. HUNGERFORD, *Algebra,* Holt, Rinehart and Winston, New York, 1974.

[566] K. HWANG, *Computer Arithmetic, Principles, Architecture and Design,* John Wiley & Sons, New York, 1979.

[567] C. I'ANSON AND C. MITCHELL, "Security defects in CCITT Recommendation X.509 – The directory authentication framework", *Computer Communication Review, 20* (1990), 30-34.

[568] R. IMPAGLIAZZO, L. LEVIN, AND M. LUBY, "Pseudo-random generation from one-way functions", *Proceedings of the 21st Annual ACM Symposium on Theory of Computing,* 12-24, 1989.

I5691 R. IMPAGLIAZZO AND M. NAOR, "Efficient cryptographic schemes provably as secure as subset sum", *Proceedings of the IEEE 30th Annual Symposium on Foundations of Computer Science, 236-241,* 1989.

[570] I. INGEMARSSON AND G.J. SIMMONS, "A protocol to set up shared secret schemes without the assistance of a mutually trusted party", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473),* 266–282, 1991.

[571] I. INGEMARSSON, D.T. TANG, AND C.K. WONG, "A conference key distribution system", *IEEE Transactions on Information Theory*, 28 (1982), 714–720.

[572] K. IRELAND AND M. ROSEN, *A Classical Introduction to Modem Number The-*ory, Springer-Verlag, New York, 2nd edition, 1990.

[573] IS0 7498-2, "Information processing systems – Open Systems Interconnection – Basic reference model – Part 2: Security architecture", International Organization for Standardization, Geneva, Switzerland, 1989 (first edition) (equivalent to ITU-T Rec. X.800).

[574] IS0 8372, "Information processing -Modes of operation for a 64-bit block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1987 (first edition; confirmed 1992).

[575] IS0 8730, "Banking – Requirements for message authentication (wholesale)", International Organization for Standardization, Geneva, Switzerland, 1990 (second edition).

[576] IS0 8731-1, "Banking – Approved algorithms for message authentication – Part 1: DEA", International Organization for Standardization, Geneva, Switzerland, 1987 (first edition; confirmed 1992).

[577] IS0 8731-2, "Banking – Approved algorithms for message authentication – Part 2: Message authenticator algorithm", International Organization for Standardization, Geneva, Switzerland, 1992 (second edition).

[578] IS0 8732, "Banking – Key management (wholesale)", International Organization for Standardization, Geneva, Switzerland, 1988 (first edition).

[623] ISO/IEC 14888-2, "Information technology -Security techniques -Digital signatures with appendix – Part 2: Identity-based mechanisms", draft (CD), 1996.

[624] ISO/IEC 14888-3, "Information technology -Security techniques -Digital signatures with appendix – Part 3: Cerificate-based mechanisms", draft (CD), 1996.

[625] M. ITO, A. SAITO, AND T. NISHIZEKI, "Secret sharing scheme realizing general access structure", *IEEE Global Telecommunications Conference*, 99-102, 1987.

[626] ITU-T REC. X.509 (REVISED), "The Directory – Authentication framework", International Telecommunication Union, Geneva, Switzerland, 1993 (equivalent to ISO/IEC 9594-8: 1995).

[627] ITU-T REC. X.509 (1988 AND 1993) TECHNICAL CORRIGENDUM 2, "The Directory – Authentication framework", International Telecommunication Union, Geneva, Switzerland, July 1995 (equivalent to Technical Corrigendum 2 to ISO/IEC 9594-8:1990&1995).

[628] ITU-T REC. X.509 (1993) AMENDMENT 1: CERTIFICATE EXTENSIONS, "The Directory – Authentication framework", International Telecommunication Union, Geneva, Switzerland, July 1995 draft for JCT1 letter ballot (equivalent to Ammendment 1 to ISO/IEC 9594-8: 1995).

[629] W.-A. JACKSON, K.M. MARTIN, AND C.M. O'KEEFE, "Multisecret threshold schemes", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 126-135, 1994.

[630] G. JAESCHKE, "On strong pseudoprimes to several bases", *Mathematics of Computation*, 61 (1993), 915-926.

[631] C.J.A. JANSEN AND D.E. BOEKEE, "On the significance of the directed acyclic word graph in cryptology", *Advances in Cryptology–AUSCRYPT '90 (LNCS 453)*, 318-326, 1990.

[632] ———, "The shortest feedback shift register that can generate a given sequence", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 90–99, 1990.

[633] T. JEBELEAN, "Comparing several gcd algorithms", *Proceedings of the 11th Symposium on Computer Arithmetic*, 180-l 85, IEEE Press, 1993.

[634] J. JEDWAB AND C. MITCHELL, "Minimum weight modified signed-digit representations and fast exponentiation", *Electronics Letters*, 25 (August 17, 1989), 1171-1172.

[635] N. JEFFERIES, C. MITCHELL, AND M. WALKER, "A proposed architecture for trusted third party services", E. Dawson and J. Golić, editors, *Cryptography: Policy and Algorithms, International Conference, Brisbane, Queensland, Australia, July 1995 (LNCS 1029)*, 98-104, 1996.

[636] H.N. JENDAL, Y.J.B. KUHN, AND J.L. MASSEY, "An information-theoretic treatment of homophonic substitution", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434)*, 382-394, 1990.

[637] S.M. JENNINGS, "Multiplexed sequences: Some properties of the minimum polynomial", *Cryptography-Proceedings of the Workshop on Cryptography, Burg Feuerstein (LNCS 149)*, 189-206, 1983.

[638] T. JOHANSSON, G. KABATIANSKII, AND B. SMEETS, "On the relation between A-codes and codes correcting independent errors", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765)*, 1–1 1, 1994.

[639] D.B. JOHNSON, A. LE, W. MARTIN, S. MATYAS, AND J. WILKINS, "Hybrid key distribution scheme giving key record recovery", *IBM Technical Disclosure Bulletin, 37* (1994), 5-16.

[640] D.B. JOHNSON AND S.M. MATYAS, "Asymmetric encryption: Evolution and enhancements", *CryptoBytes, 2* (Spring 1996), l-6.

[641] D.S. JOHNSON, "The NP-completeness column: an ongoing guide", *Journal of Algorithms, 9* (1988), 426-444.

[642] R.W. JONES, "Some techniques for handling encipherment keys", *ICL Technical Journal, 3* (1982), 175-188.

[643] R.R. JUENEMAN, "Analysis of certain aspects of output feedback mode", *Advances in Cryptology-Proceedings of Crypto 82,99*-127,1983.

[644] ———, "A high speed manipulation detection code", *Advances in Cryptology-CRYPTO '86 (LNCS 263), 327-346,* 1987.

[645] R.R. JUENEMAN, S.M. MATYAS, AND C.H. MEYER, "Message authentication with manipulation detection codes", *Proceedings of the 1983 IEEE Symposium on Security and Privacy, 33-54,* 1984.

tication using a public-key algorithm", International Organization for Standardization, Geneva, Switzerland, 1993 (first edition).

[601] ISO/IEC 9798-4, "Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function", International Organization for Standardization, Geneva, Switzerland, 1995 (first edition).

[602] ISO/IEC 9798-5, "Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero knowledge techniques", draft (CD), 1996.

[603] ISO/IEC 9979, "Data cryptographic techniques – Procedures for the registration of cryptographic algorithms", International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).

[604] ISO/IEC 10116, "Information processing – Modes of operation for an n-bit block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).

[605] ISO/IEC 10118- 1, "Information technology – Security techniques – Hash-functions – Part 1: General", International Organization for Standardization, Geneva, Switzerland, 1994.

[606] ISO/IEC 10118-2, "Information technology – Security techniques -Hash-functions -Part 2: Hash-functions using an n-bit block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1994.

[607] ISO/IEC 10118-3, "Information technology – Security techniques -Hash-functions – Part 3: Dedicated hash-functions", draft (CD), 1996.

[608] ISO/IEC 10 118-4, "Information technology – Security techniques – Hash-functions -Part 4: Hash-functions using modular arithmetic", draft (CD), 1996.

[609] I SO/IEC 10 18 1 - 1, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 1: Overview", International Organization for Standardization, Geneva, Switzerland, 1995 (equivalent to ITU-T Rec. X.810, 1995).

[610] ISO/IEC 10 18 l-2, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 2: Authentication framework", International Organization for Standardization, Geneva, Switzerland, 1995 (equivalent to ITU-T Rec. X.811, 1995).

[611] ISO/IEC 10181-3, "Information technology – Open Systems Interconnection – Security frameworks for open systems -Part 3: Access control framework", draft, 1995.

[612] ISO/IEC 10 18 1-4, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 4: Non-repudiation framework", draft, 1995.

[613] ISO/IEC 1018 1-5, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 5: Integrity framework", draft, 1995.

[614] ISO/IEC 1018 l-6, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 6: Confidentiality framework", draft, 1995.

[615] ISO/IEC 1018 l-7, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 7: Security audit framework", draft, 1995.

[616] ISO/IEC 11770- 1, "Information technology – Security techniques – Key management – Part 1: Framework", draft (DIS), 1996.

[617] ISO/IEC 11770-2, "Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques", International Organization for Standardization, Geneva, Switzerland, 1996 (first edition).

[618] ISO/IEC 11770-3, "Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques", draft (DIS), 1996.

[619] ISO/IEC 13888- 1, "Information technology – Security techniques – Non-repudiation – Part 1: General model", draft (CD), 1996.

[620] ISO/IEC 13888-2, "Information technology – Security techniques – Non-repudiation – Part 2: Using symmetric encipherment algorithms", draft (CD), 1996.

[621] ISO/IEC 13888-3, "Information technology – Security techniques – Non-repudiation – Part 3: Using asymmetric techniques", draft (CD), 1996.

[622] ISO/IEC 14888- 1, "Information technology -Security techniques -Digital signatures with appendix -Part 1: General", draft (CD), 1996.

[672] J. Kilian and P. Rogaway, "How to protect DES against exhaustive key search", *Advances in Cryptology-CRYPTO '96 (LNCS 1109)*, 252–267, 1996.

[673] S.-H. Kim and C. Pomerance, "The probability that a random probable prime is composite", *Mathematics* of *Computation, 53* (1989), 721-741.

[674] M. Kimberley, "Comparison of two statistical tests for keystream sequences", *Electronics Letters, 23* (April 9, 1987), 365-366.

[675] A. Klapper, "The vulnerability of geometric sequences based on fields of odd characteristic", *Journal of Cryptology, 7* (1994), *33-5* 1.

[676] A. Klapper and M. Goresky, "Feedback shift registers, combiners with memory, and 2-adic span", *Journal of Cryptology,* to appear.

[677] ———, "2-Adic shift registers", R. Anderson, editor, *Fast Sofhvare Encryption, Cambridge Security Workshop (LNCS 809)*, 174-178, Springer-Verlag, 1994.

[678] ———, "Cryptanalysis based on 2-adic rational approximation", *Advances in Cryptology-CRYPTO '95 (LNCS 963), 262-273, 1995.*

[679] ———, "Large period nearly de Bruijn FCSR sequences", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921), 263-273,* 1995.

[680] D.V. Klein, "Foiling the cracker: a survey of, and improvements to, password security", *Proceedings of the 2nd USENIX UNIX Security Workshop, 5-14,* 1990.

[681] H.-J. Knobloch, "A smart card implementation of the Fiat-Shamir identification scheme", Advances in *Cryptology-EUROCRYPT* '88 *(LNCS 330), 87-95, 1988.*

[682] L.R. Knudsen, "Cryptanalysis of LOKI", *Advances in Cryptology-ASIACRYPT '91 (LNCS 739), 22-35,* 1993.

[683] ———, "Cryptanalysis of LOKI91", *Advances in Cryptology–AUSCRYPT '92 (LNCS 718)*, 196–208, 1993.

[684] ———, *Block Ciphers -Analysis, Design and Applications,* PhD thesis, Computer Science Department, Aarhus University (Denmark), 1994.

[685] ——— "A key-schedule weakness in SAFER K-64": *Advances in Cryptology-CRYPTO '95 (LNCS 963)*, 274–286, 1995.

[686] ——— "Truncated and higher order differentials", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 196-211, Springer-Verlag, 1995.

[687] L.R. Knudsen and T. Berson, "Truncated differentials of SAFER", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 15-26, Springer-Verlag, 1996.

[688] L.R. Knudsen and X. Lai, "New attacks on all double block length hash functions of hash rate 1, including the parallel-DM", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950)*, 410–418, 1995.

[689] L.R. Knudsen and W. Meier, "Improved differential attacks on RC5", *Advances in Cryptology-CRYPTO '96 (LNCS 1109)*, 216–228, 1996.

[690] L.R. Knudsen and T. Pedersen, "On the difficulty of software key escrow", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070)*, 237–244, 1996.

[691] D.E. Knuth, *The Art of Computer Programming – Fundamental Algorithms,* volume 1, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1973.

[692] ———, *The Art of Computer Programming – Seminumerical Algorithms,* volume 2, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1981.

[693] ———, *The Art of Computer Programming – Sorting and* Searching, volume 3, Addison-Wesley, Reading, Massachusetts, 1973.

[694] D.E. Knuth and L. Trabb Pardo, "Analysis of a simple factorization algorithm", *Theoretical Computer Science, 3* (1976), 321-348.

[695] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation, 48* (1987), 203-209.

[696] ———, "Hyperelliptic cryptosystems", *Journal of Cryptology*, 1 (1989), 139-150.

[697] -, *A Course in Number Theory and Cryptography,* Springer-Verlag, New York, 2nd edition, 1994.

[698] C. Koç, "High-speed RSA implementation", Technical Report, RSA Laboratories, 1994.

[699] ———, "RSA hardware implementation", Technical Report TR-801, RSA Laboratories, 1996.

[646] D. JUNGNICKEL, *Finite* Fields: Structure and Arithmetics, Bibliographisches Institut – Wissenschaftsverlag, Mannheim, 1993.

[647] M. JUST, E. KRANAKIS, D. KRIZANC, AND P. VAN OORSCHOT, "On key distribution via true broadcasting", *2nd A CM Conference on Computer and Communications Security,* 81-88, ACM Press, 1994.

[648] D. KAHN, The *Codebreakers,* Macmillan Publishing Company, New York, 1967.

[649] B.S. KALISKI JR., "A chosen message attack on Demytko's elliptic curve cryptosystern", *Journal of Cryptology,* to appear.

[650] ——— "A pseudo-random bit generator based 'on elliptic logarithms", *Advances in Cryptology-CRYPTO '86 (LNCS 263),* 84–103, 1987.

[651] ———, *Elliptic curves and cryptography: a pseudorandom bit generator and other tools,* PhD thesis, MIT Department of Electrical Engineering and Computer Science, 1988.

[652] ———,"Anderson's RSA trapdoor can be broken", *Electronics Letters, 29* (July 22, 1993), 1387-1388.

[653] ———, "The Montgomery inverse and its applications", *IEEE Transactions on Computers,* 44 (1995), 1064-1065.

[654] B.S. KALISKI JR., R.L. RIVEST, AND A.T. SHERMAN, "Is the Data Encryption Standard a group? (Results of cycling experiments on DES)", *Journal of Cryptology,* 1 (1988), 3-36.

[655] B.S. KALISKI JR. AND M. ROBSHAW, "The secure use of RSA", *CryptoBytes,* 1 (Autumn 1995), 7-13.

[656] B.S. KALISKI JR. AND Y.L. YIN, "On differential and linear cryptanalysis of the RC5 encryption algorithm", *Advances in Cryptology-CRYPTO '95 (LNCS 963), 171-184,* 1995.

[657] E. KALTOFEN, "Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems", *Mathematics of Computation, 64* (1995), 777-806.

[658] E. KALTOFEN AND V. SHOUP, "Subquadratic-time factoring of polynomials over finite fields", *Proceedings of the 27th Annual ACM Symposium on Theory of Computing, 398-*406, 1995.

[659] J. KAM AND G. DAVIDA, "Structured design of substitution-permutation encryption networks", *IEEE Transactions on Computers,* 28 (1979), 747-753.

[660] N. KAPIDZIC AND A. DAVIDSON, "A certificate management system: structure, functions and protocols", *Proceedings of the Internet Society Symposium on Network and Distributed System Security,* 153-160, IEEE Computer Society Press, 1995.

[661] A. KARATSUBA AND YU. OFMAN, "Multiplication of multidigit numbers on automata", *Soviet Physics – Doklady, 7* (1963), 595-596.

[662] E.D. KARNIN, J.W. GREENE, AND M.E. HELLMAN, "On secret sharing systems", *IEEE Transactions on Information Theory, 29* (1983), 35-41.

[663] A. KEHNE, J. SCHÖWÄLDER, AND H. LANGENDÖRFER, "A nonce-based protocol for multiple authentications", *Operating Systems Review, 26* (1992), 84-89.

[664] R. KEMMERER, C. MEADOWS, AND J. MILLEN, 'Three systems for cryptographic protocol analysis", *Journal of Cryptology, 7* (1994), 79-130.

[665] S. KENT, "Encryption-based protection protocols for interactive user-computer communication", MIT/LCS/TR-162 (M.Sc. thesis), MIT Laboratory for Computer Science, 1976.

[666] ———, "Internet privacy enhanced mail", *Communications of the ACM, 36* (1993), *48-*60.

[667] ———, "Internet security standards: past, present and future", *StandardView,* 2 (1994), 78-85.

[668] A. KERCKHOFFS, "La cryptographie militaire", *Journal des Sciences Militaires,* 9th Series (February 1883), 161-191.

[669] **I. KESSLER AND H. KRAWCZYK,** "Minimum buffer length and clock rate for the shrinking generator cryptosystem", IBM Research Report RC 19938, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., 1995.

[670] E. KEY, "An analysis of the structure and complexity of nonlinear binary sequence generators", *IEEE Transactions on Information Theory, 22* (1976), 732-736.

[671] J. KILIAN AND T. LEIGHTON, "Fair cryptosystems, revisited: A rigorous approach to key-escrow", *Advances in Cryptology-CRYPTO '95 (LNCS 963),* 208-221, 1995.

[725] X. LAI, "Condition for the nonsingularity of a feedback shift-register over a general finite field", *IEEE Transactions on Information Theory, 33* (1987), 747-749.

[726] ——— "On the design and security of block 'ciphers", ETH Series in Information Processing, J.L. Massey (editor), vol. 1, Hartung-Gorre Verlag Konstanz, Technische Hochschule (Zurich), 1992.

[727] X. LAI AND L.R. KNUDSEN, "Attacks on double block length hash functions", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 157-165, Springer-Verlag, 1994.

[728] X. LAI AND J.L. MASSEY, "A proposal for a new block encryption standard", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473)*, 389–404, 1991.

[729] ———, "Hash functions based on block ciphers", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658), 55-70,* 1993.

[730] X. LAI, J.L. MASSEY, AND S. MURPHY, "Markov ciphers and differential cryptanalysis", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547)*, 17-38, 1991.

[731] X. LAI, R.A. RUEPPEL, AND J. WOOLLVEN, "A fast cryptographic checksum algorithm based on stream ciphers", *Advances in Cryptology-AUSCRYPT '92 (LNCS 718)*, 339-348, 1993.

[732] C.-S. LAIH, L. HARN, J.-Y. LEE, AND T. HWANG, "Dynamic threshold scheme based on the definition of cross-product in an n-dimensional linear space", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 286–298, 1990.

[733] C.-S. LAIH, F.-K. Tu, AND W.-C TAI, "On the security of the Lucas function", *Information Processing Letters, 53* (1995), 243-247.

[734] K.-Y. LAM AND T. BETH, 'Timely authentication in distributed systems", Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, editors, *Second European Symposium on Research in Computer Security – ESORICS'92 (LNCS 648)*, 293-303, Springer-Verlag, 1992.

[735] K.-Y. LAM AND L.C.K. HUI, "Efficiency of $SS(I)$ square-and-multiply exponentiation algorithms", *Electronics Letters, 30* (December 8, 1994), 2115-2116.

[736] B.A. LAMACCHIA AND A.M. ODLYZKO, "Computation of discrete logarithms in prime fields", *Designs, Codes and Cryptography,* 1 (1991), 47-62.

[737] ——— "Solving large sparse linear systems over finite fields", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 109-133, 1991.

[738] L. LAMPORT, "Constructing digital signatures from a one-way function", Technical report CSL-98, SRI International, Palo Alto, 1979.

[739] ———, "Password authentication with insecure communication", *Communications of the ACM, 24* (1981), 770-772.

[740] B. LAMPSON, M. ABADI, M. BURROWS, AND E. WOBBER, "Authentication in distributed systems: Theory and practice", *ACM Transactions on Computer Systems,* 10 (1992), 265-310.

[741] S.K. LANGFORD AND M.E. HELLMAN, "Differential-linear cryptanalysis", *Advances in Cryptology-CRYPTO '94 (LNCS 839)*, 17–25, 1994.

[742] P.J. LEE AND E.F. BRICKELL, "An observation on the security of McEliece's public-key cryptosystem", *Advances in Cryptology-EUROCRYPT '88 (LNCS 330), 275-280,* 1988.

[743] D.H. LEHMER, "Euclid's algorithm for large numbers", *American Mathematical Monthly,* 45 (1938), 227-233.

[744] D.H. LEHMER AND R.E. POWERS, "On factoring large numbers", *Bulletin of the AMS, 37* (193 1), 770-776.

[745] T. LEIGHTON AND S. MICALI, "Secret-key agreement without public-key cryptography", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 456-479, 1994.

[746] A.K. LENSTRA, "Posting to sci.crypt", April 11 1996.

[747] ———, "Primality testing", C. Pomerance, editor, *Cryptology and Computational Number Theory,* volume *42* of *Proceedings of Symposia in Applied Mathematics,* 13-25, American Mathematical Society, 1990.

[748] A.K. LENSTRA AND H.W. LENSTRA JR., "Algorithms in number theory", J. van Leeuwen, editor, *Handbook of Theoretical Computer Science,* 674-715, Elsevier Science Publishers, 1990.

[749] -, *The Development of the Number Field Sieve,* Springer-Verlag, Berlin, 1993.

[700] C. Koç, T. Acar, and B.S. Kaliski Jr., "Analyzing and comparing Montgomery multiplication algorithms", *IEEE Micro, 16* (1996), 26-33.

[701] J.T. Kohl, "The use of encryption in Kerberos for network authentication", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 35–43, 1990.

[702] L.M. Kohnfelder, "A method for certification", MIT Laboratory for Computer Science, unpublished (essentially pp.39-43 of [703]), 1978.

[703] ——— "Toward a practical public-key cryptosystdm", B.Sc. thesis, MIT Department of Electrical Engineering, 1978.

[704] A. Kolmogorov, "Three approaches to the definition of the concept 'quantity of information"', *Problemy Peredachi Informatsii*, 1 (1965), 3-l 1.

[705] A.G. Konheim, *Cryptography, A Primer*, John Wiley & Sons, New York, 1981.

[706] I. Koren, *Computer Arithmetic Algorithms*, Prentice Hall, Englewood Cliffs, New Jersey, 1993.

[707] V.I. Korzhik and A.I. Turkin, "Cryptanalysis of McEliece's public-key cryptosystem", *Advances in Cryptology-EUROCRYPT* '91 *(LNCS 547), 68-70,* 1991.

[708] K. Koyama, U. Maurer, T. Okamoto, and S.A. Vanstone, "New public-key schemes based on elliptic curves over the ring Z_n", *Advances in Cryptology-CRYPTO '91 (LNCS 576), 252-266,* 1992.

[709] K. Koyama and R. Terada, "How to strengthen DES-like cryptosystems against differential cryptanalysis", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science,* E76-A (1993), 63-69.

[710] E. Kranakis, *Primality and Cryptography*, John Wiley & Sons, Stuttgart, 1986.

[711] D.W. Kravitz, "Digital signature algorithm", U.S. Patent # 5,231,668, 27 Jul 1993.

[712] H. Krawczyk, "How to predict congruential generators", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 138-153, 1990.

[713] ——— "How to predict congruential generators", *journal of Algorithms,* 13 (1992), 527-545. An earlier version appeared in [712].

[714] ———, "LFSR-based hashing and authentication", *Advances in Cryptology-CRYPTO '94 (LNCS 839)*, 129-139, 1994.

[715] ———, "Secret sharing made short", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 136-146, 1994.

[716] ———, "The shrinking generator: Some practical considerations", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 45–46, Springer-Verlag, 1994.

[717] ———, "New hash functions for message authentication", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921)*, 301-310, 1995.

[718] ———, "SKEME: A versatile secure key exchange mechanism for Internet", *Proceedings of the Internet Society Symposium on Network and Distributed System Security,* 114–127, IEEE Computer Society Press, 1996.

[719] Y. Kurita and M. Matsumoto, "Primitive t-nomials (t = 3,5) over GF(2) whose degree is a Mersenne exponent $\leq$ 44497", *Mathematics of Computation, 56* (1991), 817-821.

[720] K. Kurosawa, T. Ito, and M. Takeuchi, "Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number", *Cryptologia,* 12 (1988), 225-233.

[721] K. Kurosawa, K. Okada, and S. Tsujii, "Low exponent attack against elliptic curve RSA", *Advances in Cryptology-ASIACRYPT* '94 *(LNCS 917), 376-383,* 1995.

[722] K. Kusuda and T. Matsumoto, "Optimization of time-memory trade-off cryptanalysis and its application to DES, FEAL-32, and Skipjack", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science,* E79-A (1996), 35–48.

[723] J.C. Lagarias, "Knapsack public key cryptosystems and diophantine approximation", *Advances in Cryptology-Proceedings of Crypto 83, 3-23,* 1984.

[724] ———, "Pseudorandom number generators in cryptography and number theory", C. Pomerance, editor, *Cryptology and Computational Number Theory,* volume *42* of *Proceedings of Symposia in Applied Mathematics,* 115-143, American Mathematical Society, 1990.

[776] ——— “How to construct pseudorandom permutations from pseudorandom functions”, *SIAM Journal on Computing*, 17 (1988), 373-386. An earlier version appeared in [775].

I7771 S. LUCKS, “Faster Luby-Rackoff ciphers”, D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 189-203, Springer-Verlag, 1996.

[778] F.J. MACWILLIAMS AND N.J.A. SLOANE, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977 (fifth printing: 1986).

[779] W. MADRYGA, “A high performance encryption algorithm”, J. Finch and E. Dougall, editors, *Computer Security: A Global Challenge, Proceedings of the Second IFIP International Conference on Computer Security, 557-570,* North-Holland, 1984.

I7801 D.P. MAHER, “Crypto backup and key escrow”, *Communications of the ACM, 39* (1996), 48-53.

[781] W. MAO AND C. BOYD, “On the use of encryption in cryptographic protocols”, PG. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, 251-262, Institute of Mathematics & Its Applications (IMA), 1995.

I7821 G. MARSAGLIA, “A current view of random number generation”, L. Billard, editor, *Computer Science and Statistics: Proceedings of the Sixteenth Symposium on the Interface*, 3-10, North-Holland, 1985.

[783] P. MARTIN-LÖF, “The definition of random sequences”, *Information and Control, 9* (1966), 602-619.

[784] J.L. MASSEY, “Shift-register synthesis and BCH decoding”, *IEEE Transactions on Information Theory*, 15 (1969), 122-127.

[785] ———, “An introduction to contemporary cryptology”, *Proceedings of the IEEE, 76* (1988), 533-549.

[786] ——— “Contemporary cryptology: An introduction”, G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, l-39, IEEE Press, 1992. An earlier version appeared in [785].

[787] ———, “SAFER K-64: A byte-oriented block-ciphering algorithm”, R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, l-17, Springer-Verlag, 1994.

[788] ———, “SAFER K-64: One year later”, B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 212-241, Springer-Verlag, 1995.

[789] J.L. MASSEY AND I. INGEMARSSON, “The Rip Van Winkle cipher – A simple and provably computationally secure cipher with a finite key”, *IEEE International Symposium on Information Theory (Abstracts)*, p.146, 1985.

[790] J.L. MASSEY AND X. LAI, “Device for converting a digital block and the use thereof”, European Patent # 482,154, 29 Apr 1992.

[791] ——— “Device for the conversion of a digital block and use of same”, U.S. Patent # 5,214,703, 25 May 1993.

[792] J.L. MASSEY AND J.K. OMURA, “Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission”, U.S. Patent # 4,567,600, 28 Jan 1986.

[793] J.L. MASSEY AND R.A. RUEPPEL, “Linear ciphers and random sequence generators with multiple clocks”, *Advances in Cryptology-Proceedings of EUROCRYPT84 (LNCS 209)*, 74-87, 1985.

[794] J.L. MASSEY AND S. SERCONEK, “A Fourier transform approach to the linear complexity of nonlinearly filtered sequences”, *Advances in Cryptology-CRYPTO ‘94 (LNCS 839)*, 332-340, 1994.

[795] M. MATSUI, “The first experimental cryptanalysis of the Data Encryption Standard”, *Advances in Cryptology-CRYPTO ‘94 (LNCS 839)*, l-11, 1994.

[796] ———, “Linear cryptanalysis method for DES cipher”, *Advances in Cryptology-EUROCRYPT ‘93 (LNCS 765), 386-397,* 1994.

[797] ———, “On correlation between the order of S-boxes and the strength of DES”, *Advances in Cryptology-EUROCRYPT ‘94 (LNCS 950), 366-375,* 1995.

[798] M. MATSUI AND A. YAMAGISHI, “A new method for known plaintext attack of FEAL cipher”, *Advances in Cryptology-EUROCRYPT ‘92 (LNCS 658)*, 81-91, 1993.

[799] T. MATSUMOTO AND H. IMAI, “On the key predistribution system: A practical solution to the key distribution problem”, *Advances in Cryptology-CRYPTO ‘87 (LNCS 293)*, 185–193, 1988.

[750] A.K. LENSTRA, H.W. LENSTRA JR., AND L. LOVÁSZ, "Factoring polynomials with rational coefficients", *Mathematische Annalen*, 261 (1982), 515-534.

[751] 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 (1993), 319-349.

[752] ———, "The number field sieve", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, 11-42, Springer-Verlag, 1993.

[753] A.K. LENSTRA AND M.S. MANASSE, "Factoring by electronic mail", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434)*, 355–371, 1990.

[754] "Factoring with two large primes", *Mathematics of Computation, 63* (1994), 785-798.

[755] A.K. LENSTRA, P. WINKLER, AND Y. YACOBI, "A key escrow system with warrant bounds", *Advances in Cryptology-CRYPTO* '95 *(LNCS 963)*, 197-207, 1995.

[756] H.W. LENSTRA JR., "Factoring integers with elliptic curves", *Annals of Mathematics*, 126 (1987), 649-673.

[757] ———, "Finding isomorphisms between finite fields", *Mathematics of Computation, 56* (1991), 329-347.

[758] ———, "On the Chor-Rivest knapsack cryptosystem", *Journal of Cryptology, 3* (1991), 149-155.

[759] H.W. LENSTRA JR. AND C. POMERANCE, "A rigorous time bound for factoring integers", *Journal of the American Mathematical Society*, 5 (1992). 483-5 16.

[760] H.W. LENSTRA JR. AND R.J. SCHOOF, "Primitive normal bases for finite fields", *Mathematics of Computation, 48* (1987), 217-231.

[761] L.A. LEVIN, "One-way functions and pseudorandom generators", *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 363-365,* 1985.

[762] J. LEVINE, *United States Cryptographic Patents 1861-1981,* Cryptologia, Inc., Terre Haute, Indiana, 1983.

[763] R. LIDL AND W.B. MÜLLER, "Permutation polynomials in RSA-cryptosystems", *Advances in Cryptology-Proceedings of Crypto 83*, 293–301, 1984.

[764] R. LIDL AND H. NIEDERREITER, *Finite Fields,* Cambridge University Press, Cambridge, 1984.

[765] A. LIEBL, "Authentication in distributed systems: A bibliography", *Operating Systems Review, 27* (1993), 31-41.

[766] C.H. LIM AND P.J. LEE, "Another method for attaining security against adaptively chosen ciphertext attacks", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 420–434, 1994.

[767] ———, "More flexible exponentiation with precomputation", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 95-107, 1994.

[768] ———, "Server (prover/signer)-aided verification of identity proofs and signatures", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921), 64-78,* 1995.

[769] S. LIN AND D. COSTELLO, *Error Control Coding: Fundamentals and Applications,* Prentice Hall, Englewood Cliffs, New Jersey, 1983.

[770] J. LIPSON, *Elements of Algebra and Algebraic Computing,* Addison-Wesley, Reading, Massachusetts, 198 1.

[771] T.M.A. LOMAS, L. GONG, J.H. SALTZER, AND R.M. NEEDHAM, "Reducing risks from poorly chosen keys", *Operating Systems Review, 23* (Special issue), 14-18. (Presented at: 12th ACM Symposium on Operating Systems Principles, Litchfield Park, Arizona, Dec. 1989).

[772] D.L. LONG AND A. WIGDERSON, "The discrete logarithm hides O(log n) bits", *SIAM Journal on Computing,* 17 (1988), 363-372.

[773] R. LOVORN, *Rigorous, subexponential algorithms for discrete logarithms over finite jields,* PhD thesis, University of Georgia, 1992.

[774] M. LUBY, *Pseudorandomness and Cryptographic Applications,* Princeton University Press, Princeton, New Jersey, 1996.

[775] M. LUBY AND C. RACKOFF, "Pseudorandom permutation generators and cryptographic composition", *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, 356-363,* 1986.

[826] ———, “Cryptographic key distribution and computation in class groups”, R.A. Mollin, editor, *Number Theory and Applications*, 459–479, Kluwer Academic Publishers, 1989.

[827] ——— “The discrete logarithm problem”, C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, 49-74, American Mathematical Society, 1990.

[828] R.J. McEliece, “A public-key cryptosystem based on algebraic coding theory”, DSN progress report 42-44, Jet Propulsion Laboratory, Pasadena, 1978.

[829] ———, *The Theory of Information and Coding: A Mathematical Frameworkfor Communication*, Cambridge University Press, Cambridge, 1984.

[830] ———, *Finite Fields for Computer Scientists and Engineeers*, Kluwer Academic Publishers, Boston, 1987.

[831] C.A. Meadows, “Formal verification of cryptographic protocols: a survey”, *Advances in Cryptology-ASIACRYPT ‘94 (LNCS 917)*, 133–150, 1995.

[832] W. Meier, “On the security of the IDEA block cipher”, *Advances in Cryptology–EUROCRYPT ‘93 (LNCS 765)*, *371-385*, 1994.

[833] W. Meier and 0. Staffelbach, “Fast correlation attacks on stream ciphers”, *Advances in Cryptology-EUROCRYPT ‘88 (LNCS 330)*, 301-314, 1988.

[834] ———, “Fast correlation attacks on certain stream ciphers”, *Journal of Cryptology*, 1 (1989), 159-176. An earlier version appeared in [833].

[835] ———, “Analysis of pseudo random sequences generated by cellular automata”, *Advances in Cryptology-EUROCRYPT ‘91 (LNCS 547)*, 186-199, 1991.

[836] ———, “Correlation properties of combiners with memory in stream ciphers”, *Advances in Cryptology-EUROCRYPT ‘90 (LNCS 473)*, 204213, 1991.

[837] ——— “Correlation properties of combiners with memory in stream ciphers”, *Journal of Cryptology, 5* (1992), 67-86. An earlier version appeared in [836].

[838] ——— “The self-shrinking generator”, *Advances’ in Cryptology-EUROCRYPT ‘94 (LNCS 950)*. 205-214. 1995.

[839] S. Mendes and C. Huitema, “A new approach to the X.509 framework: allowing a global authentication infrastructure without a global trust model”, *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, 172-189, IEEE Computer Society Press, 1995.

[840] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston, 1993.

[841] A. Menezes, I. Blake, X. Gao, R. Mullin, S. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publishers, Boston, 1993.

[842] A. Menezes, T. Okamoto, and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field”, *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 80-89*, 1991.

[843] ——— “Reducing elliptic curve logarithms to logarithms in a finite field”, *IEEE Transactions on Information Theory, 39* (1993), 1639-1646. An earlier version appeared in [842].

[844] A. Menezes, M. Qu, and S. Vanstone, “Some new key agreement protocols providing implicit authentication”, workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC’95), Ottawa, Canada, May 18-19 1995.

[845] R. Menicocci, “Cryptanalysis of a two-stage Gollmann cascade generator”, W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 62-69*, 1993.

[846] R.C. Merkle, “Digital signature system and method based on a conventional encryption function”, U.S. Patent # 4,881,264, 14 Nov 1989.

[847] ———, “Method and apparatus for data encryption”, U.S. Patent # 5,003,597, 26 Mar 1991.

[848] ———, “Method of providing digital signatures”, U.S. Patent # 4,309,569, 5 Jan 1982.

[849] ———, “Secure communications over insecure channels”, *Communications of the ACM*, 21 (1978), 294–299.

[850] ———, *Secrecy, Authentication, and Public Key Systems*, UMI Research Press, Ann Arbor, Michigan, 1979.

[800] T. MATSUMOTO, Y. TAKASHIMA, AND H. IMAI, "On seeking smart public-key-distribution systems", *The Transactions of the IECE of Japan,* E69 (1986), 99-106.

[801] S.M. MATYAS, "Digital signatures – an overview", *Computer Networks, 3* (1979), 87-94.

[802] ———, "Key handling with control vectors", *IBM Systems Journal, 30* (1991), 151-174.

[803] ———, "Key processing with control vectors", *Journal of Cryptology, 3* (1991), 113-136.

[804] S.M. MATYAS AND C.H. MEYER, "Generation, distribution, and installation of cryptographic keys", *IBM Systems Journal,* 17 (1978), 126-137.

[805] S.M. MATYAS, C.H. MEYER, AND J. OSEAS, "Generating strong one-way functions with cryptographic algorithm", *IBM Technical Disclosure Bulletin, 27* (1985), 5658–5659.

[806] S.M. MATYAS, C.H.W. MEYER, AND B.O. BRACHTL, "Controlled use of cryptographic keys via generating station established control values", U.S. Patent # 4,850,017, 18 Jul 1989.

[807] U. MAURER, "Fast generation of secure RSA-moduli with almost maximal diversity", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434), 636-647,* 1990.

[808] ——— "New approaches to the design of self-synchronizing stream ciphers", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547),* 458-471, 1991.

[809] ———, "A provably-secure strongly-randomized cipher", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473),* 361-373, 1991.

[810] ———, "A universal statistical test for random bit generators", *Advances in Cryptology-CRYPTO '90 (LNCS 537), 409-420,* 1991.

[811] ——— "Conditionally-perfect secrecy and a provably-secure randomized cipher", *Journal of Cryptology, 5 (1992), 53-66.* An earlier version appeared in [809].

[812] ———, "Some number-theoretic conjectures and their relation to the generation of cryptographic primes", C. Mitchell, editor, *Cryptography and Coding* II, volume *33* of *Institute of Mathematics & Its Applications (IMA),* 173–19 1, Clarendon Press, 1992.

[813] ———, "A universal statistical test for random bit generators", *Journal of Cryptology, 5* (1992). 89-105. An earlier version appeared in [810].

[814] ———, "Factoring with an oracle", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658),* 429436, 1993.

[815] -, "Secret key agreement by public discussion from common information", *IEEE Transactions on Information Theory, 39* (1993), 733-742.

[816] ———, "A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658), 239-255,* 1993.

[817] ———, "Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms", *Advances in Cryptology-CRYPTO '94 (LNCS 839),* 271-281, 1994.

[818] ———, "Fast generation of prime numbers and secure public-key cryptographic parameters", *Journal of Cryptology, 8* (1995), 123-155. An earlier version appeared in [807].

[819] ——— "The role of information theory in cryptography", PG. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV, 49-*71, Institute of Mathematics & Its Applications (IMA), 1995.

[820] U. MAURER AND J.L. MASSEY, "Perfect local randomness in pseudo-random sequences", *Advances in Cryptology-CRYPTO* '89 *(LNCS 435),* 100-112, 1990.

[821] ———, "Local randomness in pseudorandom sequences", *Journal of Cryptology, 4* (1991), 135-149. An earlier version appeared in [820].

[822] ———, "Cascade ciphers: The importance of being first", *Journal of Cryptology, 6* (1993), 55-61.

[823] U. MAURER AND Y. YACOBI, "Non-interactive public-key cryptography", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547), 498-507,* 1991.

[824] ———, "A remark on a non-interactive public-key distribution system", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658),* 458–460, 1993.

[825] K.S. MCCURLEY, "A key distribution system equivalent to factoring", *Journal of Cryptology,* 1 (1988), 95-105.

[877] S.P. Miller, B.C. Neuman, J.I. Schiller, and J.H. Saltzer, "Kerberos authentication and authorization system", Section E.2.1 of Project Athena Technical Plan, MIT, Cambridge, Massachusetts, 1987.

[878] V. S. Miller, "Use of elliptic curves in cryptography", *Advances in Cryptology-CRYPTO '85 (LNCS 218)*, 417426, 1986.

[879] C. Mitchell, "A storage complexity based analogue of Maurer key establishment using public channels", C. Boyd, editor, *Cryptography and Coding, 5th IMA Conference, Proceedings, 84-93,* Institute of Mathematics & Its Applications (IMA), 1995.

[880] ———, "Limitations of challenge-response entity authentication", *Electronics Letters, 25* (August 17, 1989), 1195-1196.

[881] C. Mitchell and F. Piper, "Key storage in secure networks", *Discrete Applied Mathematics,* 21 (1988), 215-228.

[882] C. Mitchell, F. Piper, and P. Wild, "Digital signatures", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity, 325-378,* IEEE Press, 1992.

[883] A. Mitropoulos and H. Meijer, "Zero knowledge proofs – a survey", Technical Report No. 90-IR-05, Queen's University at Kingston, Kingston, Ontario, Canada, 1990.

[884] S. Miyaguchi, "The FEAL cipher family", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 627-638, 1991.

[885] S. Miyaguchi, S. Kurihara, K. Ohta, and H. Morita, "Expansion of FEAL cipher", *NTT Review, 2* (1990), 117-127.

[886] S. Miyaguchi, K. Ohta, and M. Iwata, "128-bit hash function (N-hash)", *NTT Review, 2* (1990), 128-132.

[887] S. Miyaguchi, A. Shiraishi, and A. Shimizu, "Fast data encipherment algorithm FEAL-8", *Review of the Electrical Communications Laboratories, 36* (1988), 433-437.

[888] A. Miyaji and M. Tatebayashi, "Public key cryptosystem with an elliptic curve", U.S. Patent # 5,272,755, 21 Dec 1993.

[889] ——— "Method of privacy communication using elliptic curves", U.S. Patent # 5,351,297, 27 Sep 1994 (continuation-in-part of 5,272,755).

[890] S.B. Mohan and B.S. Adiga, "Fast algorithms for implementing RSA public key cryptosystem", *Electronics Letters,* 21 (August 15, 1985), 761.

[891] R. Molva, G. Tsudik, E. Van Herreweghen, and S. Zatti, "KryptoKnight authentication and key distribution system", Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, editors, *Second European Symposium on Research in Computer Security – ESORICS'92 (LNCS 648),* 155-174, Springer-Verlag, 1992.

[892] L. Monier, "Evaluation and comparison of two efficient probabilistic primality testing algorithms", *Theoretical Computer Science,* 12 (1980), 97-108.

[893] P. Montgomery, "Modular multiplication without trial division", *Mathematics of Computation, 44* (1985), 5 19-521.

[894] ———, "Speeding the Pollard and elliptic curve methods of factorization", *Mathematics of Computation, 48* (1987), 243-264.

[895] P. Montgomery and R. Silverman, "An FFT extension to the $P - 1$ factoring algorithm", *Mathematics of Computation, 54* (1990), 839-854.

[896] P.L. Montgomery, "A block Lanczos algorithm for finding dependencies over $GF(2)$", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921)*, 106-120, 1995.

[897] A.M. Mood, 'The distribution theory of runs", *The Annals of Mathematical Statistics,* 11 (1940), 367-392.

[898] J.H. Moore, "Protocol failures in cryptosysterns", *Proceedings of the IEEE, 76* (1988), 594-602.

[899] ———, "Protocol failures in cryptosystems", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 541-558, IEEE Press, 1992. Appeared earlier as [898].

[900] 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,* 13 (1987), 262-273. An earlier version appeared in [901].

[901] ———, "Cycle structure of the DES with weak and *semi-weak* keys", *Advances in Cryptology-CRYPTO '86 (LNCS 263), 9-32,* 1987.

[851] ——, "Secrecy, authentication, and public key systems", Technical Report No. 1979-1, Information Systems Laboratory, Stanford University, Palo Alto, California, 1979. Also available as [850].

[852] ——, "Protocols for public key cryptosysterns", *Proceedings of the 1980 IEEE Symposium on Security and Privacy*, 122–134, 1980.

[853] —— "A certified digital signature", *Advance; in Cryptology-CRYPTO '89 (LNCS 435)*, 218-238, 1990.

[854] ——, "A fast software one-way hash function", *Journal of Cryptology*, *3* (1990), 43-58.

[855] "One way hash functions and DES", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 428-446, 1990.

[856] "Fast software encryption functions", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 476-501, 1991.

[857] R.C. MERKLE AND M.E. HELLMAN, "Hiding information and signatures in trapdoor knapsacks", *IEEE Transactions on Information Theory*, *24* (1978), 525-530.

[858] ——, "On the security of multiple encryption", *Communications of the ACM*, *24* (1981), 465–467.

[859] C.H. MEYER AND S.M. MATYAS, *Cryptography: A New Dimension in Computer Data Security*, John Wiley & Sons, New York, 1982 (third printing).

[860] C.H. MEYER AND M. SCHILLING, "Secure program load with manipulation detection code", *Proceedings of the 6th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'88)*, 111-130, 1988.

[861] S. MICALI, "Fair cryptosystems and methods of use", U.S. Patent # 5,276,737, 4 Jan 1994.

[862] —— "Fair cryptosystems and methods of use", U.S. Patent # 5,315,658, 24 May 1994 (continuation-in-part of 5,276,737).

[863] ——, "Fair public-key cryptosystems", *Advances in Cryptology-CRYPTO '92 (LNCS 740)*, 113-138, 1993.

[864] S. MICALI, 0. GOLDREICH, AND S. EVEN, "On-line/off-line digital signing", U.S. Patent # 5,016,274, 14 May 1991.

[865] S. MICALI, C. RACKOFF, AND B. SLOAN, 'The notion of security for probabilistic cryptosystems", *SIAM Journal on Computing*, 17 (1988), 412-426.

[866] S. MICALI AND C.P. SCHNORR, "Efficient, perfect random number generators", *Advances in Cryptology-CRYPTO '88 (LNCS 403)*, 173-198, 1990.

[867] ——, "Efficient, perfect polynomial random number generators", *Journal of Cryptology*, *3* (1991), 157-172. An earlier version appeared in [866].

[868] S. MICALI AND A. SHAMIR, "An improvement of the Fiat-Shamir identification and signature scheme", *Advances in Cryptology-CRYPTO '88 (LNCS 403)*, 244–247, *1990.*

[869] S. MICALI AND R. SIDNEY, "A simple method for generating and sharing pseudo-random functions, with applications to Clipper-like key escrow systems", *Advances in Cryptology-CRYPTO '95 (LNCS 963)*, 185-196, 1995.

[870] P. MIHAILESCU, "Fast generation of provable primes using search in arithmetic progressions", *Advances in Cryptology-CRYPTO '94 (LNCS 839), 282-293,* 1994.

[871] M.J. MIHALJEVIĆ, "A security examination of the self-shrinking generator", presentation at 5th IMA Conference on Cryptography and Coding, Cirencester, U.K., December 1995.

[872] ——, "An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure", *Advances in Cryptology-AUSCRYPT '92 (LNCS 718), 349-356, 1993.*

[873] ——, "A correlation attack on the binary sequence generators with time-varying output function", *Advances in Cryptology-ASIACRYPT '94 (LNCS 917), 67-79,* 1995.

[874] M.J. MIHALJEVIĆ AND J.D. GOLIĆ, "A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence", *Advances in Cryptology-AUSCRYPT '90 (LNCS 453)*, 165-175, 1990.

[875] ——, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658)*, 124-137, 1993.

[876] G.L. MILLER, "Riemann's hypothesis and tests for primality", *Journal of Computer and System Sciences*, 13 (1976), 300-3 17.

[926] B.C. NEUMAN AND T. Ts'o, "Kerberos: an authentication service for computer networks", *IEEE Communications Magazine, 32* (September 1994), 33-38.

[927] H. NIEDERREITER, 'The probabilistic theory of linear complexity", *Advances in Cryptology-EUROCRYPT '88 (LNCS 330)*, 191-209, 1988.

[928] ——, "A combinatorial approach to probabilistic results on the linear-complexity profile of random sequences", *Journal of Cryptology*, 2 (1990), 105-112.

[929] ——, "Keystream sequences with a good linear complexity profile for every starting point", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434), 523-532,* 1990.

[930] —— "The linear complexity profile and the jump complexity of keystream sequences", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473)*, 174-188, 1991.

[931] K. NISHIMURA AND M. SIBUYA, "Probability to meet in the middle", *Journal of Cryptology*, 2 (1990), 13-22.

[932] I.M. NIVEN AND H.S. ZUCKERMAN, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 4th edition, 1980.

[933] M.J. NORRIS AND G.J. SIMMONS, "Algorithms for high-speed modular arithmetic", *Congressus Numerantium*, 31 (1981), 153-163.

19341 G. NORTON, "Extending the binary gcd algorithm", J. Calmet, editor, *Algebraic Algorithms and Error-Correcting Codes, 3rd International Conference, AAECC-3 (LNCS 229)*, 363-372, Springer-Verlag, 1986.

[935] K. NYBERG, "On one-pass authenticated key establishment schemes", workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC'95), Ottawa, Canada, May 18-19 1995.

[936] K. NYBERG AND R. RUEPPEL, "A new signature scheme based on the DSA giving message recovery", *1st ACM Conference on Computer and Communications Security*, 58-61, ACM Press, 1993.

[937] ——, "Weaknesses in some recent key agreement protocols", *Electronics Letters, 30* (January 6, 1994), 26-27.

[938] ——, "Message recovery for signature schemes based on the discrete logarithm problem", *Designs, Codes and Cryptography, 7* (1996), 61-81.

[939] A.M. ODLYZKO, "Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme", *IEEE Transactions on Information Theory, 30* (1984), 594-601.

[940] ——, "Discrete logarithms in finite fields and their cryptographic significance", *Advances in Cryptology-Proceedings of EUROCRYPT84 (LNCS 209)*, 224-314, 1985.

[941] ——, "The rise and fall of knapsack cryptosystems", C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, 75-88, American Mathematical Society, 1990.

[942] ——, "Discrete logarithms and smooth polynomials", G.L. Mullen and P.J-S. Shiue, editors, *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemporary Mathematics*, 269-278, American Mathematical Society, 1994.

[943] K. OHTA AND K. AOKI, "Linear cryptanalysis of the Fast Data Encipherment Algorithm", *Advances in Cryptology-CRYPTO '94 (LNCS 839)*, 12-16, 1994.

[944] K. OHTA AND T. OKAMOTO, "Practical extension of Fiat-Shamir scheme", *Electronics Letters, 24* (July 21, 1988), 955-956.

[945] ——, "A modification of the Fiat-Shamir scheme", *Advances in Cryptology-CRYPTO* '88 *(LNCS 403), 232-243,* 1990.

[946] E. OKAMOTO AND K. TANAKA, "Key distribution system based on identification information", *IEEE Journal on Selected Areas in Communications, 7* (1989), 481-485.

[947] T. OKAMOTO, "A single public-key authentication scheme for multiple users", *Systems and Computers in Japan*, 18 (1987), 14-24. Translated from *Denshi Tsushin Gakkai Ronbunshi* vol. 69-D no.10, October 1986, 1481-1489.

[948] ——, "A fast signature scheme based on congruential polynomial operations", *IEEE Transactions on Information Theory, 36* (1990), 47-53.

[949] —— "Provably secure and practical identification schemes and corresponding signature

[902] F. MORAIN, "Distributed primality proving and the primality of $(2^{3539}+1)/3$", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473)*, 110-123, 1991.

I9031 ———, "Prime values of partition numbers and the primality of $p_{1840926}$", LIX Research Report LIX/RR/92/11, Laboratoire d'Informatique de l'Ecole Polytechnique, France, June 1992.

[904] F. MORAIN AND J. OLIVOS, "Speeding up the computations on an elliptic curve using addition-subtraction chains", *Theoretical Informatics and Applications, 24* (1990), 531–543.

[905] I.H. MORGAN AND G.L. MULLEN, "Primitive normal polynomials over finite fields", *Mathematics of Computation, 63* (1994), 759–765.

[906] R. MORRIS, "The Hagelin cipher machine (M-209), Reconstruction of the internal settings", *Cryptologia, 2* (1978), 267-278.

[907] R. MORRIS AND K. THOMPSON, "Password security: a case history", *Communications of the ACM, 22* (1979), 594-597.

[908] M.A. MORRISON AND J. BRILLHART, "A method of factoring and the factorization of F_7", *Mathematics of Computation, 29* (1975), 183-205.

[909] W.B. MÜLLER AND R. NÖBAUER, "Cryptanalysis of the Dickson-scheme", *Advances in Cryptology-EUROCRYPT '85 (LNCS 219)*, 50-61, 1986.

I9101 W.B. MÜLLER AND W. NÖBAUER, "Some remarks on public-key cryptosystems", *Studia Scientiarum Mathematicarum Hungarica,* 16 (1981), 71-76.

[911] R. MULLIN, I. ONYSZCHUK, S. VANSTONE, AND R. WILSON, "Optimal normal bases in $GF(p^n)$", *Discrete Applied Mathematics, 22* (1988/89), 149-161.

[912] S. MUND, "Ziv-Lempel complexity for periodic sequences and its cryptographic application", *Advances in Cryptology-EUROCRYPT* '91 *(LNCS 547)*, 114-126, 1991.

[913] S. MURPHY, "The cryptanalysis of FEAL-4 with 20 chosen plaintexts", *Journal of Cryptology, 2* (1990), 145-154.

[914] D. NACCACHE, "Can O.S.S. be repaired? – proposal for a new practical signature scheme", *Advances in Cryptology-EUROCRYPT* '93 *(LNCS 765), 233-239,* 1994.

[915] D. NACCACHE, D. M'RAÏHI, AND D. RAPHAELI, "Can Montgomery parasites be avoided? A design methodology based on key and cryptosystem modifications", *Designs, Codes and Cryptography, 5* (1995), 73-80.

[916] D. NACCACHE, D. M'RAÏHI, S. VAUDENAY, AND D. RAPHAELI, "Can D.S.A. be improved? Complexity trade-offs with the digital signature standard", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950)*, 77–85, 1995.

[917] D. NACCACHE AND H. M'SILTI, "A new modulo computation algorithm", *Recherche Opérationnelle – Operations Research (RAIRO-OR), 24* (1990), 307-313.

[918] K. NAGASAKA, J.-S. SHIUE, AND C.-W. HO, "A fast algorithm of the Chinese remainder theorem and its application to Fibonacci number", G.E. Bergum, A.N. Philippou, and A.F. Horadam, editors, *Applications of Fibonacci Numbers, Proceedings of the Fourth International Conference on Fibonacci Numbers and their Applications, 24* l-246, Kluwer Academic Publishers, 1991.

[919] M. NAOR AND A. SHAMIR, "Visual cryptography", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 1-12, 1995.

[920] M. NAOR AND M. YUNG, "Universal one-way hash functions and their cryptographic applications", *Proceedings of the 21st Annual ACM Symposium on Theory of Computing,* 33–43, 1989.

[921] ———, "Public-key cryptosystems provably secure against chosen ciphertext attacks", *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing,* 427–437, 1990.

[922] J. NECHVATAL, "Public key cryptography", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 177-288, IEEE Press, 1992.

[923] R.M. NEEDHAM AND M.D. SCHROEDER, "Using encryption for authentication in large networks of computers", *Communications of the ACM,* 21 (1978), 993-999.

[924] ———, "Authentication revisited", *Operating Systems Review,* 21 (1987), 7.

[925] B.C. NEUMAN AND S.G. STUBBLEBINE,"A note on the use of timestamps as nonces", *Operating Systems Review, 27* (1993), 10–14.

[974] R. PINCH, “The Carmichael numbers up to 10^{15}”, *Mathematics of Computation*, 61 (1993), 381-391.

I9751 ——— “Some primality testing algorithms”, *Notice; of the American Mathematical Society*, 40 (1993), 1203-1210.

[976] ———, “Extending the Håstad attack to LUC”, *Electronics Letters*, 31 (October 12, 1995), 1827-1828.

[977] ———, “Extending the Wiener attack to RSA-type cryptosystems”, *Electronics Letters, 3* 1 (September 28, 1995), 1736-1738.

I9781 V. PLESS, “Encryption schemes for computer confidentiality”, *IEEE Transactions on Computers, 26* (1977), 1133-1136.

[979] J.B. PLUMSTEAD, “Inferring a sequence generated by a linear congruence”, *Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science*, 153-159, 1982.

I9801 ——— “Inferring a sequence produced by a linear congruence”, *Advances in Cryptology–Proceedings of Crypto 82*, 317–319, 1983.

[981] H.C. POCKLINGTON, “The determination of the prime or composite nature of large numbers by Fermat’s theorem”, *Proceedings of the Cambridge Philosophical Society*, 18 (1914), 29-30.

I9821 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* (1978), 106-110.

[983] D. POINTCHEVAL, “A new identification scheme based on the perceptrons problem”, *Advances in Cryptology-EUROCRYPT ‘95 (LNCS 921)*, 319-328, 1995.

I9841 J.M. POLLARD, “Theorems on factorization and primality testing”, *Proceedings of the Cambridge Philosophical Society, 76* (1974), 521-528.

[985] ———, “A Monte Carlo method for factorization”, *BIT*, 15 (1975), 331-334.

[986] ———, “Monte Carlo methods for index computation (mod *p)“, Mathematics of Computation, 32* (1978), 918-924.

[987] ———, “Factoring with cubic integers”, A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, 4–10, Springer-Verlag, 1993.

[988] J.M. POLLARD AND C. SCHNORR, “An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$”, *IEEE Transactions on Information Theory, 33* (1987), 702-709.

[989] C. POMERANCE, “Analysis and comparison of some integer factoring algorithms”, H.W. Lenstra Jr. and R. Tijdeman, editors, *Computational Methods in Number Theory, Part I*, 89-139, Mathematisch Centrum, 1982.

[990] ———, “The quadratic sieve factoring algorithm”, *Advances in Cryptology-Proceedings of EUROCRYPT 84 (LNCS 209)*, 169-182, 1985.

I9911 ———, “Fast, rigorous factorization and discrete logarithm algorithms”, *Discrete Algorithms and Complexity*, 119-143, Academic Press, 1987.

[992] ——— “Very short primality proofs”, *Mathematics’of Computation, 48* (1987), 3 15-322.

[993] ———, editor, *Cryptology and Computational Number Theory*, American Mathematical Society, Providence, Rhode Island, 1990.

[994] ———, “Factoring”, C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume *42* of *Proceedings of Symposia in Applied Mathematics*, 27–47, American Mathematical Society, 1990.

I9951 ———, “The number field sieve”, W. Gautschi, editor, *Mathematics of Computation, 1943-1993: A Half-Century of Computation Mathematics*, volume *48* of *Proceedings of Symposia in Applied Mathematics*, 465–480, American Mathematical Society, 1994.

I9961 C. POMERANCE, J.L. SELFRIDGE, AND S. S. WAGSTAFF JR., “The pseudoprimes to $25 \cdot 10^9$”, *Mathematics of Computation, 35* (1980), 1003-1026.

I9971 C. POMERANCE AND J. SORENSON, “Counting the integers factorable via cyclotomic methods”, *Journal of Algorithms*, 19 (1995), 250-265.

I9981 G.J. POPEK AND C.S. KLINE, “Encryption and secure computer networks”, *ACM Computing Surveys*, 11 (1979), 33 l-356.

I9991 E. PRANGE, “An algorithm for factoring $x^n - 1$ over a finite field”, AFCRC-TN-59-775, Air Force Cambridge Research Center, 1959.

[1000] V.R. PRATT, “Every prime has a succinct certificate”, *SIAM Journal on Computing, 4* (1975), 214-220.

schemes", *Advances in Cryptology-CRYPTO* '92 *(LNCS 740)*, 31-53, 1993.

[950] ———, "Designated confirmer signatures and public-key encryption are equivalent", *Advances in Cryptology-CRYPTO '94 (LNCS 839)*, 61-74, 1994.

[951] ———, "An efficient divisible electronic cash scheme", *Advances in Cryptology-CRYPTO* '95 *(LNCS 963)*, 438–451, 1995.

[952] T. OKAMOTO, S. MIYAGUCHI, A. SHIRAISHI, AND T. KAWAOKA, "Signed document transmission system", U.S. Patent # 4,625,076, 25 Nov 1986.

[953] T. OKAMOTO AND A. SHIRAISHI, "A fast signature scheme based on quadratic inequalities", *Proceedings of the 1985 IEEE Symposium on Security and Privacy*, 123–132, 1985.

[954] T. OKAMOTO, A. SHIRAISHI, AND T. KAWAOKA, "Secure user authentication without password files", Technical Report NI83-92, I.E.C.E., Japan, January 1984. In Japanese.

[955] J. OLIVOS, "On vectorial addition chains", *Journal of Algorithms*, 2 (1981), 13-21.

[956] J.K. OMURA AND J.L. MASSEY, "Computational method and apparatus for finite field arithmetic", U.S. Patent # 4,587,627, 6 May 1986.

[957] H. ONG AND C.P. SCHNORR, "Fast signature generation with a Fiat Shamir-like scheme", *Advances in Cryptology-EUROCRYPT* '90 *(LNCS 473), 432-440, 1991.*

[958] H. ONG, C.P. SCHNORR, AND A. SHAMIR, "An efficient signature scheme based on quadratic equations", *Proceedings of the 16th Annual ACM Symposium on Theory of Computing*, 208-216, 1984.

[959] I.M. ONYSZCHUK, R.C. MULLIN, AND S.A. VANSTONE, "Computational method and apparatus for finite field multiplication", U.S. Patent # 4,745,568, 17 May 1988.

[960] G. ORTON, "A multiple-iterated trapdoor for dense compact knapsacks", *Advances in Cryptology-EUROCRYPT '94 (LNCS 950)*, 112-130, 1995.

[961] D. OTWAY AND 0. REES, "Efficient and timely mutual authentication", *Operating Systems Review*, 21 (1987), 8-10.

[962] J.C. PAILLÈS AND M. GIRAULT, "CRIPT: A public-key based solution for secure data communications", *Proceedings of the 7th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'89)*, 171-185, 1989.

[963] C.H. PAPADIMITRIOU, *Computational Complexity*, Addison-Wesley, Reading, Massachusetts, 1994.

[964] S.-J. PARK, S.-J. LEE, AND S.-C. GOH, "On the security of the Gollmann cascades", *Advances in Cryptology-CRYPTO '95 (LNCS 963)*, 148-156, 1995.

[965] J. PATARIN, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070), 33-48, 1996.*

[966] J. PATARIN AND P. CHAUVAUD, "Improved algorithms for the permuted kernel problem", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 391-402, 1994.

[967] W. PENZHORN AND G. KÜHN, "Computation of low-weight parity checks for correlation attacks on stream ciphers", C. Boyd, editor, *Cryptography and Coding, 5th IMA Conference, Proceedings*, 74-83, Institute of Mathematics & Its Applications (IMA), 1995.

[968] R. PERALTA, "Simultaneous security of bits in the discrete log", *Advances in Cryptology–EUROCRYPT '85 (LNCS 219), 62-72,* 1986.

[969] R. PERALTA AND V. SHOUP, "Primality testing with fewer random bits", *Computational Complexity*, 3 (1993), 355-367.

[970] A. PFITZMANN AND R. ASSMANN, "More efficient software implementations of (generalized) DES", *Computers & Security*, 12 (1993), 477-500.

[971] B. PFITZMANN AND M. WAIDNER, "Fail-stop signatures and their applications", *Proceedings of the 9th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'91)*, 145-160, 1991.

[972] ———, "Formal aspects of fail-stop signatures", Interner Bericht 22/90, Universität Karlsruhe, Germany, December 1990.

[973] S.J.D. PHOENIX AND P.D. TOWNSEND, "Quantum cryptography: protecting our future networks with quantum mechanics", C. Boyd, editor, *Cryptography and Coding, 5th IMA Conference, Proceedings*, 112-1 3 I, Institute of Mathematics & Its Applications (IMA), 1995.

[1027] ——, "Efficient dispersal of information for security, load balancing, and fault tolerance", *Journal of the Association for Computing Machinery, 36* (1989), 335-348.

[1028] T. Rabin and M. Ben-Or, "Verifiable secret sharing and multiparty protocols with honest majority", *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, 73-85*, 1989.

[1029] C. Rackoff and D.R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack", *Advances in Cryptology-CRYPTO '91 (LNCS 576)*, 433-444, 1992.

[1030] G. Rawlins, *Compared to What? An Introduction to the Analysis of Algorithms*, Computer Science Press, New York, 1992.

[1031] G. Reitwiesner, "Binary arithmetic", *Advances in Computers*, 1 (1960), 23 l-308.

[1032] T. Renji, "On finite automaton one-key cryptosystems", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 135-148, Springer-Verlag, 1994.

[1033] RFC 13 19, '"The MD2 message-digest algorithm", Internet Request for Comments 1319, B. Kaliski, April 1992 (updates RFC 1115, August 1989, J. Linn).

034] RFC 1320, "The MD4 message-digest algorithm", Internet Request for Comments 1320, R.L. Rivest, April 1992 (obsoletes RFC 1186, October 1990, R. Rivest).

035] RFC 132 1, "The MD5 message-digest algorithm", Internet Request for Comments 1321, R.L. Rivest, April 1992 (presented at Rump Session of Crypto'91).

[1036] RFC 142 1, "Privacy enhancement for Internet electronic mail – Part I: Message encryption and authentication procedures", Internet Request for Comments 1421, J. Linn, February 1993 (obsoletes RFC 1113 – September 1989; RFC 1040 – January 1988; and RFC 989 -February 1987, J. Linn).

[1037] RFC 1422, "Privacy enhancement for Internet electronic mail -Part II: Certificate-based key management", Internet Request for Comments 1422, S. Kent, February 1993 (obsoletes RFC 1114, August 1989, S. Kent and J. Linn).

[1038] RFC 1423, "Privacy enhancement for Internet electronic mail – Part III: Algorithms, modes, and identifiers", Internet Request for Comments 1423, D. Balenson, February 1993 (obsoletes RFC 1115, September 1989, J. Linn).

[1039] RFC 1424, "Privacy enhancement for Internet electronic mail – Part IV: Key certification and related services", Internet Request for Comments 1424, B. Kaliski, February 1993.

[1040] RFC 1508, "Generic security service application program interface", Internet Request for Comments 1508, J. Linn, September 1993.

[1041] RFC 1510, "The Kerberos network authentication service (V5)", Internet Request for Comments 1510, J. Kohl and C. Neuman, September 1993.

[1042] RFC 1521, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for specifying and describing the format of Internet message bodies", Internet Request for Comments 1521, N. Borenstein and N. Freed, September 1993 (obsoletes RFC 1341).

[1043] RFC 1750, "Randomness requirements for security", Internet Request for Comments 1750, D. Eastlake, S. Crocker and J. Schiller, December 1994.

[1044] RFC 1828, "IP authentication using keyed MD5", Internet Request for Comments 1828, P. Metzger and W. Simpson, August 1995.

[1045] RFC 1847, "Security multiparts for MIME: Multipart/signed and multipart/encrypted", Internet Request for Comments 1847, J. Galvin, S. Murphy, S. Crocker and N. Freed, October 1995.

[1046] RFC 1848, "MIME object security services", Internet Request for Comments 1848, S. Crocker, N. Freed, J. Galvin and S. Murphy, October 1995.

[1047] RFC 1938, "A one-time password system", Internet Request for Comments 1938, N. Haller and C. Metz, May 1996.

[1048] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De Win, "The cipher SHARK", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 99-l 11, Springer-Verlag, 1996.

[1049] V. Rijmen and B. Preneel, "On weaknesses of non-surjective round functions", presented at the 2nd Workshop on Selected Areas in Cryptography (SAC'95), Ottawa, Canada, May 18-19 1995.

[1001] B. PRENEEL, "Standardization of cryptographic techniques", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 162-173, Springer-Verlag, 1993.

[1002] ——, "Cryptographic hash functions", *European Transactions on Telecommunications*, 5 (1994), 431-448.

[1003] ——, *Analysis and design of cryptographic hash functions*, PhD thesis, Katholieke Universiteit Leuven (Belgium), Jan. 1993.

[1 0 0 4 1 - t *Cryptographic Hash Functions*, Kluwer Academic Publishers, Boston, (to appear). Updated and expanded from [1003].

[1005] B. PRENEEL, R. GOVAERTS, AND J. VANDEWALLE, "Differential cryptanalysis of hash functions based on block ciphers", *1st ACM Conference on Computer and Communications Security*, 183-188, ACM Press, 1993.

[1006] ——, "Information authentication: Hash functions and digital signatures", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 87-131, Springer-Verlag, 1993.

[1007] ——, "Hash functions based on block ciphers: A synthetic approach", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 368–378, 1994.

[1008] B. PRENEEL, M. NUTTIN, V. RIJMEN, AND J. BUELENS, "Cryptanalysis of the CFB mode of the DES with a reduced number of rounds", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 212-223, 1994.

[1009] B. PRENEEL AND P. VAN OORSCHOT, "MDx-MAC and building fast MACs from hash functions", *Advances in Cryptology-CRYPTO '9.5 (LNCS 963)*, 1-14, 1995.

[1010] ——, "On the security of two MAC algorithms", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070)*, 19–32, 1996.

[loll] N. PROCTOR, "A self-synchronizing cascaded cipher system with dynamic control of error propagation", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196)*, 174-190, 1985.

[1012] G.B. PURDY, "A high security log-in procedure", *Communications of the ACM*, 17 (1974), 442445.

[1013] M. QU AND S.A. VANSTONE, 'The knapsack problem in cryptography", *Contemporary Mathematics*, 168 (1994), 291-308.

[1014] K. QUINN, "Some constructions for key distribution patterns", *Designs, Codes and Cryptography*, 4 (1994), 177-191.

[1015] J.-J. QUISQUATER, "A digital signature scheme with extended recovery", preprint, 1995.

[1016] J.-J. QUISQUATER AND C. COUVREUR, "Fast decipherment algorithm for RSA public-key cryptosystem", *Electronics Letters*, 18 (October 14, 1982), 905-907.

[1017] J.-J. QUISQUATERAND J.-P. DELESCAILLE, "How easy is collision search? Application to DES", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434)*, 429–434, 1990.

[1018] ——, "How easy is collision search. New results and applications to DES", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 408–413, 1990.

[1019] J.-J. QUISQUATER AND M. GIRAULT, "2n-bit hash-functions using n-bit symmetric block cipher algorithms", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434)*, 102–109, 1990.

[1020] J.-J. QUISQUATER, L. GUILLOU, AND T. BERSON, "How to explain zero-knowledge protocols to your children", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, *628-*631, 1990.

[1021] M.O. RABIN, "Probabilistic algorithms", J.F. Traub, editor, *Algorithms and Complexity*, 21–40, Academic Press, 1976.

[1022] ——, "Digitalized signatures", R. DeMillo, D. Dobkin, A. Jones, and R. Lipton, editors, *Foundations of Secure Computation*, 155–168, Academic Press, 1978.

[1023] —— "Digitalized signatures and public-key functions as intractable as factorization", MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[1024] ——, "Probabilistic algorithm for testing primality", *Journal of Number Theory*, 12 (1980), 128-138.

[1025] ——, "Probabilistic algorithms in finite fields", *SIAM Journal on Computing, 9* (1980), 273-280.

[1026] ——, "Fingerprinting by random polynomials", TR-15-8 1, Center for Research in Computing Technology, Harvard University, 198 1.

[1077] ———, "Linear complexity and random sequences", *Advances in Cryptology-EUROCRYPT '85 (LNCS 219)*, 167-188, 1986.

[1078] ———, "Key agreements based on function composition", *Advances in Cryptology-EUROCRYPT '88 (LNCS 330)*, 3-10, 1988.

[1079] ———, "On the security of Schnorr's pseudo random generator", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434), 423-428,* 1990.

[1080] ———, "A formal approach to security architectures", *Advances in Cryptology-EUROCRYPT '91 (LNCS 547), 387-398,* 1991.

[1081] ———, "Stream ciphers", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 65-134, IEEE Press, 1992.

[1082] ———,"Criticism of ISO CD 11166 banking — key management by means of asymmetric algorithms", W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy*, 191-198, 1993.

[1083] R.A. RUEPPEL, A. LENSTRA, M. SMID, K.MCCURLEY, Y.DESMEDT, A.ODLYZKO, AND P. LANDROCK, "The Eurocrypt '92 controversial issue: trapdoor primes and moduli", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658)*, 194-199, 1993.

[1084] R.A. RUEPPEL AND J.L. MASSEY, "The knapsack as a non-linear function", *IEEE International Symposium on Information Theory (Abstracts)*, p.46, 1985.

[1085] R.A. RUEPPEL AND O.J. STAFFELBACH, "Products of linear recurring sequences with maximum complexity", *IEEE Transactions on Information Theory, 33* (1987), 124-I 3 1.

[1086] R.A. RUEPPEL AND P.C. VAN OORSCHOT, "Modem key agreement techniques", *Computer Communications*, 17 (1994), 458-465.

[1087] A. RUSSELL, "Necessary and sufficient conditions for collision-free hashing", *Advances in Cryptology-CRYPTO '92 (LNCS 740)*, 433–441, 1993.

[1088] ———, "Necessary and sufficient conditions for collision-free hashing", *Journal of Cryptology*, 8 (1995), 87-99. An earlier version appeared in [1087].

[1089] A. SALOMAA, *Public-key Cryptography*, Springer-Verlag, Berlin, 1990.

[1090] M. SANTHA AND U.V. VAZIRANI, "Generating quasi-random sequences from slightly-random sources", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, 434-440,* 1984.

[1091] ———, "Generating quasi-random sequences from semi-random sources", *Journal of Computer and System Sciences, 33* (1986), 75-87. An earlier version appeared in [1090].

[10921 0. SCHIROKAUER, "Discrete logarithms and local units", *Philosophical Transactions of the Royal Society of London A, 345* (1993), 409-423.

[1093] B. SCHNEIER, "Description of a new variable-length key, 64-bit block cipher (Blowfish)", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 191-204, Springer-Verlag, 1994.

[1094] ———, *Applied Cryptography: Protocols, Algorithms, and Source Code in* C, John Wiley & Sons, New York, 2nd edition, 1996.

[1095] C.P. SCHNORR, "Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system", U.S. Patent # 4,995,082, 19 Feb 1991.

[1096] ———, "On the construction of random number generators and random function generators", *Advances in Cryptology-EUROCRYPT '88 (LNCS 330), 225-232,* 1988.

[1097] ———, "Efficient identification and signatures for smart cards", *Advances in Cryptology-CRYPTO '89 (LNCS 435), 239-252, 1990.*

[1098] ———, "Efficient signature generation by smart cards", *Journal of Cryptology, 4* (1991), 161-174.

[1099] C.P. SCHNORR AND M. EUCHNER, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems", L. Budach, editor, *Fundamentals of Computation Theory (LNCS 529)*, 68-85, Springer-Verlag, 1991.

[1100] C.P. SCHNORR AND H.H. HÖRNER, "Attacking the Chor-Rivest cryptosystem by improved lattice reduction", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921)*, 1-12, 1995.

[1101] A. SCHÖNAGE, "A lower bound for the length of addition chains", *Theoretical Computer Science*, 1 (1975), 1-12.

[1050] ———, "Improved characteristics for differential cryptanalysis of hash functions based on block ciphers", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 242-248, Springer-Verlag, 1995.

[1051] R.L. RIVEST, "Are 'strong' primes needed for RSA?", Unpublished manuscript, 1991.

[1052] ———, "Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem", *Cryptologia, 2* (1978), 62-65.

[1053] ———, "Statistical analysis of the Hagelin cryptograph", *Cryptologia, 5* (1981), 27-32.

[1054] ———, "Cryptography", J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, 719-755, Elsevier Science Publishers, 1990.

[1055] ———, "The MD4 message digest algorithm", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 303-311, 1991.

[1056] ——— "The RC5 encryption algorithm", B. Preheel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 86-96, Springer-Verlag, 1995.

[1057] R.L. RIVEST AND A. SHAMIR, "How to expose an eavesdropper", *Communications of the ACM, 27* (1984), 393-395.

[1058] ———, "Efficient factoring based on partial information", *Advances in Cryptology-EUROCRYPT '85 (LNCS 219), 31-34*, 1986.

[1059] R.L. RIVEST, A. SHAMIR, AND L.M. ADLEMAN, "Cryptographic communications system and method", U.S. Patent # 4,405,829, 20 Sep 1983.

[1060] ———, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM,* 21 (1978), 120-126.

[1061] R.L. RIVEST AND A.T. SHERMAN, "Randomized encryption techniques", *Advances in Cryptology-Proceedings of Crypto 82,* 145–163, 1983.

[1062] M.J.B. ROBSHAW, "On evaluating the linear complexity of a sequence of least period 2^n", *Designs, Codes and Cryptography, 4* (1994), 263-269.

[1063] ———, "Stream ciphers", Technical Report TR-701 (version 2.0), RSA Laboratories, 1995.

[1064] M. ROE, "How to reverse engineer an EES device", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 305-328, Springer-Verlag, 1995.

[1065] P. ROGAWAY, "Bucket hashing and its application to fast message authentication", *Advances in Cryptology-CRYPTO '95 (LNCS 963)*, 29-42, 1995.

[1066] P. ROGAWAY AND D. COPPERSMITH, "A software-optimized encryption algorithm", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 56-63, Springer-Verlag, 1994.

[1067] N. ROGIER AND P. CHAUVAUD, 'The compression function of MD2 is not collision free", workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC'95), Ottawa, Canada, May 18-19 1995.

[1068] J. ROMPEL, "One-way functions are necessary and sufficient for secure signatures", *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, 387-394,* 1990.

[1069] K.H. ROSEN, *Elementary Number Theory and its Applications*, Addison-Wesley, Reading, Massachusetts, 3rd edition, 1992.

[1070] J. ROSSER AND L. SCHOENFELD, "Approximate formulas for some functions of prime numbers", *Illinois Journal of Mathematics, 6* (1962), 64-94.

[1071] RSA LABORATORIES, "The Public-Key Cryptography Standards – PKCS #1 1: Cryptographic token interface standard", RSA Data Security Inc., Redwood City, California, April 28 1995.

[1072] ———, "The Public-Key Cryptography Standards (PKCS)", RSA Data Security Inc., Redwood City, California, November 1993 Release.

[1073] A.D. RUBIN AND P. HONEYMAN, "Formal methods for the analysis of authentication protocols", CITI Technical Report 93-7, Information Technology Division, University of Michigan, 1993.

[1074] F. RUBIN, "Decrypting a stream cipher based on J-K flip-flops", *IEEE Transactions on Computers, 28* (1979), 483–487.

[1075] R.A. RUEPPEL, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, 1986.

[1076] ——— "Correlation immunity and the summation generator", *Advances in Cryptology-CRYPTO '85 (LNCS 218), 260-272,* 1986.

[1129] V. SHOUP, “New algorithms for finding irreducible polynomials over finite fields”, *Mathematics of Computation, 54* (1990), 435-447.

[1130] ——, “Searching for primitive roots in finite fields”, *Mathematics of Computation, 58* (1992), 369-380.

[1131] ——, “Fast construction of irreducible polynomials over finite fields”, *Journal of Symbolic Computation,* 17 (1994), 371-391.

[1132] T. SIEGENTHALER, “Correlation-immunity of nonlinear combining functions for cryptographic applications”, *IEEE Transactions on Information Theory, 30* (1984), 776–780.

[1133] ——, “Decrypting a class of stream ciphers using ciphertext only”, *IEEE Transactions on Computers, 34* (1985), 81-85.

[1134] ——, “Cryptanalysts representation of nonlinearly filtered ML-sequences”, *Advances in Cryptology-EUROCRYPT ‘85 (LNCS 219),* 103-110, 1986.

[1135] R.D. SILVERMAN, “The multiple polynomial quadratic sieve”, *Mathematics of Computation, 48* (1987), 329-339.

[1136] R.D. SILVERMAN AND S.S. WAGSTAFF JR., “A practical analysis of the elliptic curve factoring algorithm”, *Mathematics of Computation, 6* 1 (1993), 445-462.

[1137] G.J. SIMMONS, “A “weak” privacy protocol using the RSA crypto algorithm”, *Cryptologia, 7* (1983), 180-182.

[1138] ——, “Authentication theory/coding theory”, *Advances in Cryptology-Proceedings of CRYPTO* 84 *(LNCS 196),* 411431, 1985.

[1139] ——, “The subliminal channel and digital signatures”, *Advances in Cryptology-Proceedings of EUROCRYPT84 (LNCS 209),* 364-378, 1985.

[1140] —— “A secure subliminal channel (?)”, *Advances’ in Cryptology-CRYPTO ‘8.5 (LNCS 218),* 33-41, 1986.

[1141] —— “How to (really) share a secret”, *Advances’ in Cryptology-CRYPTO ‘88 (LNCS 403),* 390–448, 1990.

[1142] ——, “Prepositioned shared secret and/or shared control schemes”, *Advances in Cryptology-EUROCRYPT ‘89 (LNCS 434),* 436-467, 1990.

[1143] ——, “Contemporary cryptology: a foreword”, G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* vii-xv, IEEE Press, 1992.

[1144] —— “A survey of information authentication”, ‘G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 379-419, IEEE Press, 1992.

[1145] ——, “An introduction to shared secret and/or shared control schemes and their application”, G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 441-497, IEEE Press, 1992.

[1146] —— “How to insure that data acquired to verify treaty compliance are trustworthy”, G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 6 15-630, IEEE Press, 1992.

[1147] ——, ‘The subliminal channels in the U.S. Digital Signature Algorithm (DSA)“, W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 35-54,* 1993.

[1148] ——, “Proof of soundness (integrity) of cryptographic protocols”, *Journal of Cryptology,* 7 (1994), 69-77.

[1149] ——, “Subliminal communication is easy using the DSA”, *Advances in Cryptology-EUROCRYPT ‘93 (LNCS 765),* 218-232, 1994.

[1150] ——, “Protocols that ensure fairness”, P.G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV,* 383-394, Institute of Mathematics & Its Applications (IMA), 1995.

[1151] G.J. SIMMONS AND M.J. NORRIS, “Preliminary comments on the M.I.T. public-key cryptosystem”, *Cryptologiu,* 1 (1977), 406-414.

[1152] A. SINKOV, *Elementary Cryptanalysis: A Mathematical Approach,* Random House, New York, 1968.

[11153] M.E. SMID, “Integrating the Data Encryption Standard into computer networks”, *IEEE Transactions on Communications, 29* (1981), 762-772.

[1154] M.E. SMID AND D.K. BRANSTAD, “Cryptographic key notarization methods and apparatus”, U.S. Patent # 4,386,233, 31 May 1983.

[1155] ——, “The Data Encryption Standard: Past and future”, *Proceedings of the IEEE, 76* (1988), 550-559.

[1156] ——, “The Data Encryption Standard: Past and future”, G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 43-64, IEEE Press, 1992. Appeared earlier as [1155].

[1102] A.W. Schrift and A. Shamir, "On the universality of the next bit test", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 394–408, 1991.

[1103] ———, "Universal tests for nonuniform distributions", *Journal of Cryptology, 6* (1993), 119-133. An earlier version appeared in [1102].

[1104] F. Schwenk and J. Eisfeld, "Public key encryption and signature schemes based on polynomials over $\mathbb{Z}_n$", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070)*, 60–71, 1996.

[1105] R. Sedgewick, *Algorithms*, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1988.

[1106] R. Sedgewick, T.G. Szymanski, and A.C. Yao, 'The complexity of finding cycles in periodic functions", *SIAM Journal on Computing*, 11 (1982), 376-390.

[1107} E. S. Selmer, "Linear recurrence relations over finite fields", Department of Mathematics, University of Bergen, Norway, 1966.

[1108] J. Shallit, "On the worst case of three algorithms for computing the Jacobi symbol", *Journal of Symbolic Computation*, 10 (1990), 593-610.

1093 A. Shamir, "A fast signature scheme", MIT/LCS/TM-107, MIT Laboratory for Computer Science, 1978.

110] ———, "How to share a secret", *Communications of the ACM, 22* (1979), 612-613.

[1111] ———, "On the generation of cryptographically strong pseudo-random sequences", S. Even and 0. Kariv, editors, *Automata, Languages, and Programming, 8th Colloquium (LNCS 115), 544-550*, Springer-Verlag, 1981.

[1112] ———, "On the generation of cryptographically strong pseudorandom sequences", *ACM Transactions on Computer Systems*, 1 (1983), 38–44. An earlier version appeared in [1111].

[1113] ———, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem", *Advances in Cryptology-Proceedings of Crypto 82*, 279–288, 1983.

[1114] ———, "A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem", *IEEE Transactions on Information Theory, 30* (1984), 699-704. An earlier version appeared in [1113].

[1115] ——— "Identity-based cryptosystems and signature schemes", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196), 47-*53, 1985.

[1116] ———, "An efficient identification scheme based on permuted kernels", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 606–609, 1990.

[1117] ——— "RSA for paranoids", *CryptoBytes*, 1 (Autumn 1995), 1–4.

[1118] A. Shamir and A. Fiat, "Method, apparatus and article for identification and signature", U.S. Patent # 4,748,668, 31 May 1988.

[1119] M. Shand and J. Vuillemin, "Fast implementations of RSA cryptography", *Proceedings of the 11th IEEE Symposium on Computer Arithmetic, 252-259*, 1993.

[1120] C.E. Shannon, "A mathematical theory of communication", *Bell System Technical Journal, 27* (1948), 379-423, 623-656.

[1121] ———, "Communication theory of secrecy systems", *Bell System Technical Journal, 28* (1949), 656-715.

[1122] ———, "Prediction and entropy of printed English", *Bell System Technical Journal, 30* (1951), 50-64.

[1123] J. Shawe-Taylor, "Generating strong primes", *Electronics Letters, 22* (July 31, 1986), 875-877.

[1124] S. Shepherd, "A high speed software implementation of the Data Encryption Standard", *Computers & Security*, 14 (1995), 349-357.

[11251 A. Shimizu and S. Miyaguchi, "Data randomization equipment", U.S. Patent # 4,850,019, 18 Jul 1989.

[1126] ———, "Fast data encipherment algorithm FEAL", *Advances in Cryptology-EUROCRYPT '87 (LNCS 304), 267-278*, 1988.

[1127] Z. Shmuely, "Composite Diffie-Hellman public-key generating systems are hard to break", Technical Report #356, TECHNION – Israel Institute of Technology, Computer Science Department, 1985.

[1128] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", *Proceedings of the IEEE 35th Annual Symposium on Foundations of Computer Science*, 124-134, 1994.

[1183] P. SYVERSON AND P. VAN OORSCHOT, "On unifying some cryptographic protocol logics", *Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy,* 14-28, 1994.

[1184] K. TANAKA AND E. OKAMOTO, "Key distribution using id-related information directory suitable for mail systems", *Proceedings of the 8th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'90),* 115-122, 1990.

[1185] A. TARAH AND C. HUITEMA, "Associating metrics to certification paths", Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, editors, *Second European Symposium on Research in Computer Security – ESORICS'92 (LNCS 648),* 175-189, Springer-Verlag, 1992.

[1186] J.J. TARDO AND K. ALAGAPPAN, "SPX: Global authentication using public key certificates", *Proceedings of the IEEE Symposium on Research in Security and Privacy, 232-*244, 1991.

[1187] A. TARDY-C• RFDIR AND H. GILBERT, "A known plaintext attack of PEAL-4 and FEAL-6", *Advances in Cryptology-CRYPTO '91 (LNCS 576),* 172-182, 1992.

[1188] M. TATEBAYASHI, N. MATSUZAKI, AND D.B. NEWMAN JR., "Key distribution protocol for digital mobile communication systems", *Advances in Cryptology-CRYPTO '89 (LNCS 435), 324-334,* 1990.

[1189] R. TAYLOR, "An integrity check value algorithm for stream ciphers", *Advances in Cryptology-CRYPTO '93 (LNCS 773),* 40–48, 1994.

[1190] J.A. THIONG LY, "A serial version of the Pohlig-Hellman algorithm for computing discrete logarithms", *Applicable Algebra in Engineering, Communication and Computing, 4* (1993), 77–80.

[1191] J. THOMPSON, "S/MIME message specification – PKCS security services for MIME", RSA Data Security Inc., Aug. 29 1995, `http://www.rsa.com/`.

[1192] T. TOKITA, T. SORIMACHI, AND M. MATSUI, "Linear cryptanalysis of LOKI and s^2DES", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917), 293-303,* 1995.

[1193] ——, "On applicability of linear cryptanalysis to DES-like cryptosystems – LOK189, LOK19 1 and s^2DES", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science,* E78-A (1995), 1148-1153. An earlier version appeared in [1192].

[1194] M. TOMPA AND H. WOLL, "Random self-reducibility and zero-knowledge interactive proofs of possession of information", *Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science, 472-*482, 1987.

[1195] ——, "How to share a secret with cheaters", *Journal of Cryptology,* 1 (1988), 133-138.

[1196] G. TSUDIK, "Message authentication with one-way hash functions", *Computer Communication Review, 22* (1992), 29-38.

[197] S. TSUJII AND J. CHAO, "A new ID-based key sharing system", *Advances in Cryptology-CRYPTO '91 (LNCS 576), 288-*299, 1992.

:1198] W. TUCHMAN, "Integrated system design", D.K. Branstad, editor, *Computer security and the Data Encryption Standard, 94-96,* NBS Special Publication 500-27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.

[1199] ——, "Hellman presents no shortcut solutions to the DES", *IEEE Spectrum,* 16 (1979), 40–41.

[1200] J. VAN DE GRAAF AND R. PERALTA, "A simple and secure way to show the validity of your public key", *Advances in Cryptology–CRYPTO '87 (LNCS 293),* 128-134, 1988.

[1201] E. VAN HEIJST, T.P. PEDERSEN, AND B. PFITZMANN, "New constructions of fail-stop signatures and lower bounds", *Advances in Cryptology-CRYPTO '92 (LNCS 740),* 15-30, 1993.

[1202] E. VAN HEYST AND T.P. PEDERSEN, "How to make efficient fail-stop signatures", *Advances in Cryptology-EUROCRYPT '92 (LNCS 658), 366-377,* 1993.

[1203] P. VAN OORSCHOT, "A comparison of practical public key cryptosystems based on integer factorization and discrete logarithms", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity,* 289-322, IEEE Press, 1992.

[1204] ——, "Extending cryptographic logics of belief to key agreement protocols", *1st ACM Conference on Computer and Communications Security, 232-243,* ACM Press, 1993.

[1157] ——, "Response to comments on the NIST proposed digital signature standard", *Advances in Cryptology-CRYPTO '92 (LNCS 740)*, 76-88, 1993.

[1158] D.R. Smith and J.T. Palmer, "Universal fixed messages and the Rivest-Shamir-Adleman cryptosystem", *Mathematika, 26* (1979), 44-52.

[1159] J.L. Smith, "Recirculating block cipher cryptographic system", U.S. Patent # 3,796,830, 12 Mar 1974.

[1160] ——, "The design of Lucifer: A cryptographic device for data communications", IBM Research Report RC 3326, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Apr. 15 1971.

[1161] P. Smith and M. Lennon, "LUC: A new public key system", E. Dougall, editor, *Proceedings of the IFIP TC11 Ninth International Conference on Information Security, IFIP/Sec* 93, 103-l 17, North-Holland, 1993.

[1162] P. Smith and C. Skinner, "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms", *Advances in Cryptology-ASIACRYPT '94 (LNCS 917)*, 357–364, 1995.

[1163] R. Solovay and V. Strassen, "A fast Monte-Carlo test for primality", *SIAM Journal on Computing,* 6 (1977), 84-85. Erratum in ibid, 7 (1978), 118.

[1164] J. Sorenson, "Two fast gcd algorithms", *Journal of Algorithms,* 16 (1994), 110–144.

[1165] A. Sorkin, "Lucifer, a cryptographic algorithm", *Cryptologia, 8* (1984), 22-35.

[1166] M. Stadler, J.-M. Piveteau, and J. Camenisch, "Fair blind signatures", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921)*, 209-219, 1995.

[1167] 0. Staffelbach and W. Meier, "Cryptographic significance of the carry for ciphers based on integer addition", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 601-614, 1991.

[1168] W. Stahnke, "Primitive binary polynomials", *Mathematics of Computation, 27* (1973), *977-980.*

[1169] D.G. Steer, L. Strawczynski, W. Diffie, and M. Wiener, "A secure audio teleconference system", *Advances in Cryptology-CRYPTO '88 (LNCS 403), 520-528,* 1990.

[1170] J. Stein, "Computational problems associated with Racah algebra", *Journal of Computational Physics,* 1 (1967), 397405.

[1171] J.G. Steiner, C. Neuman, and J.I. Schiller, "Kerberos: an authentication service for open network systems", *Proceedings of the Winter 1988 Usenix Conference,* 19 1–201, 1988.

[1172] M. Steiner, G. Tsudik, and M. Waidner, "Refinement and extension of encrypted key exchange", *Operating Systems Review,* 29:3 (1995), 22-30.

[1173] J. Stern, "Secret linear congruential generators are not cryptographically secure", *Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science,* 421-426, 1987.

[1174] ——, "An alternative to the Fiat-Shamir protocol", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 173-180, 1990.

[1175] ——, "Designing identification schemes with keys of short size", *Advances in Cryptology-CRYPTO '94 (LNCS 839)*, 164–173, 1994.

[1176] ——, "A new identification scheme based on syndrome decoding", *Advances in Cryptology-CRYPTO '93 (LNCS 773)*, 13-21, 1994.

[1177] D.R. Stinson, "An explication of secret sharing schemes", *Designs, Codes and Cryptography, 2* (1992), 357-390.

[1178] —— *Cryptography: Theory and Practice,* CRC Press, Boca Raton, Florida, 1995.

[1179] S.G. Stubblebineand V.D. Gligor, "On message integrity in cryptographic protocols", *Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy,* 85-104, 1992.

[1180] D.J. Sykes, "The management of encryption keys", D.K. Branstad, editor, *Computer security and the Data Encryption Standard, 46-53,* NBS Special Publication 500-27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.

[1181] P. Syverson, "Knowledge, belief and semantics in the analysis of cryptographic protocols", *Journal of Computer Security,* 1 (1992), 317-334.

[1182] ——, "A taxonomy of replay attacks", *Proceedings of the Computer Security Foundations Workshop VII (CSFW 1994)*, 187-191, IEEE Computer Society Press, 1994.

[1229] S.T. WALKER, S.B. LIPNER, C.M. ELLISON, AND D.M. BALENSON, "Commercial key recovery", *Communications of the ACM*, 39 (1996), 41–47.

[1230] C.D. WALTER, "Faster modular multiplication by operand scaling", *Advances in Cryptology-CRYPTO '91 (LNCS 576)*, 3 13–323, 1992.

[1231] P.C. WAYNER, "Content-addressable search engines and DES-like systems", *Advances in Cryptology-CRYPTO '92 (LNCS 740)*, 575–586, 1993.

[1232] D. WEBER, "An implementation of the general number field sieve to compute discrete logarithms mod p", *Advances in Cryptology-EUROCRYPT '95 (LNCS 921)*, 95–105, 1995.

[1233] A.F. WEBSTER AND S.E. TAVARES, "On the design of S-boxes", *Advances in Cryptology-CRYPTO '85 (LNCS 218), 523-534*, 1986.

[1234] M.N. WEGMAN AND J.L. CARTER, "New hash functions and their use in authentication and set equality", *Journal of Computer and System Sciences, 22* (1981), 265-279.

[1235] D. WELSH, *Codes and Cryptography*, Clarendon Press, Oxford, 1988.

[1236] A.E. WESTERN AND J.C.P. MILLER, *Tables of Indices and Primitive Roots*, volume 9, Royal Society Mathematical Tables, Cambridge University Press, 1968.

[1237] D.J. WHEELER, "A bulk data encryption algorithm", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 127-134, Springer-Verlag, 1994.

[1238] D.J. WHEELER AND R.M. NEEDHAM, "TEA, a tiny encryption algorithm", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008), 363-*366, Springer-Verlag, 1995.

[1239] D.H. WIEDEMANN, "Solving sparse linear equations over finite fields", *IEEE Transactions on Information Theory, 32* (1986), 54–62.

[1240] M.J. WIENER, "Cryptanalysis of short RSA secret exponents", *IEEE Transactions on Information Theory, 36* (1990), 553-558.

[1241] ———, "Efficient DES key search", Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, 1994. Presented at Crypto '93 rump session.

[1242] S. WIESNER, "Conjugate coding", *SIGACT* News, 15 (1983), 78-88. Original manuscript (*cira* 1970).

[1243] H.S. WILF, "Backtrack: An O(1) expected time algorithm for the graph coloring problem", *Information Processing Letters,* 18 (1984), 119-121.

[1244] M.V. WILKES, *Time-Sharing Computer Systems,* American Elsevier Pub. Co., New York, 3rd edition, 1975.

[1245] F. WILLEMS, "Universal data compression and repetition times", *IEEE Transactions on Information Theory, 35* (1989), 54-58.

[1246] H.C. WILLIAMS, "A modification of the RSA public-key encryption procedure", *IEEE Transactions on Information Theory, 26* (1980), 726-729.

[1247] ———,"A p + 1 method of factoring", *Mathematics of Computation, 39* (1982), 225-234.

[1248] ———, "Some public-key Crypto-functions as intractable as factorization", *Cryptologia, 9* (1985), 223-237.

[1249] H.C. WILLIAMS AND B. SCHMID, "Some remarks concerning the M.I.T. public-key cryptosystem", *BIT,* 19 (1979), 525-538.

[1250] R.S. WINTERNITZ, "A secure one-way hash function built from DES", *Proceedings of the 1984 IEEE Symposium on Security and Privacy, 88-90,* 1984.

[1251] S. WOLFRAM, "Cryptography with cellular automata", *Advances in Cryptology-CRYPTO '85 (LNCS 218), 429-432,* 1986.

[1252] ———, "Random sequence generation by cellular automata", *Advances in Applied Mathematics, 7* (1986), 123-169.

[1253] H. WOLL, "Reductions among number theoretic problems", *Information and Computation, 72* (1987), 167-179.

[1254] A.D. WYNER, "The wire-tap channel", *Bell System Technical Journal, 54* (1975), 1355–1387.

[1255] Y. YACOBI, "A key distribution "paradox"", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 268-273, 1991.

[1256] Y. YACOBI AND Z. SHMUELY, "On key distribution systems", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 344–355, 1990.

[1257] A.C. YAO, "On the evaluation of powers", *SIAM Journal on Computing, 5* (1976). 100–103.

[1205] ———, "An alternate explanation of two BAN-logic "failures"", *Advances in Cryptology-EUROCRYPT '93 (LNCS 765)*, 443–447, 1994.

[1206] P. VAN OORSCHOT AND M. WIENER, "A known-plaintext attack on two-key triple encryption", *Advances in Cryptology-EUROCRYPT '90 (LNCS 473)*, 318–325, 1991.

[1207] ———, "Parallel collision search with applications to hash functions and discrete logarithms", *2nd ACM Conference on Computer and Communications Security*, 210-218, ACM Press, 1994.

[1208] ——— "Improving implementable meet-in-the-mihdle attacks by orders of magnitude", *Advances in Cryptology-CRYPTO '96 (LNCS 1109)*, 229-236, 1996.

[1209] ———, "On Diffie-Hellman key agreement with short exponents", *Advances in Cryptology-EUROCRYPT '96 (LNCS 1070)*, 332–343, 1996.

[1210] H.C.A. VAN TILBORG, *An Introduction to Cryptology*, Kluwer Academic Publishers, Boston, 1988.

[1211] ———, "Authentication codes: an area where coding and cryptology meet", C. Boyd, editor, *Cryptography and Coding, 5th IMA Conference, Proceedings*, 169-183, Institute of Mathematics & Its Applications (IMA), 1995.

[1212] J. VAN TILBURG, "On the McEliece public-key cryptosystem", *Advances in Cryptology-CRYPTO* '88 *(LNCS 403)*, 119-131, 1990.

[1213] S.A. VANSTONE AND R.J. ZUCCHERATO, "Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbb{Z}_n$", *IEEE Transactions on Information Theory*, to appear.

[1214] ———, "Short RSA keys and their generation", *Journal of Cryptology, 8* (1995), 101–114.

[1215] S. VAUDENAY, "On the need for multipermutations: Cryptanalysis of MD4 and SAFER", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 286-297, Springer-Verlag, 1995.

[1216] ———, "On the weak keys of Blowfish", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 27-32, Springer-Verlag, 1996.

[1217] U.V. VAZIRANI, "Towards a strong communication complexity theory, or generating quasi-random sequences from two communicating slightly-random sources", *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 366-378*, 1985.

[1218] U.V. VAZIRANI AND V.V. VAZIRANI, "Efficient and secure pseudo-random number generation", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science*, 458–463, 1984. This paper also appeared in [1219].

[1219] ———, "Efficient and secure pseudo-random number generation", *Advances in Cryptology-Proceedings of CRYPTO 84 (LNCS 196)*, 193-202, 1985.

[1220] K. VEDDER, "Security aspects of mobile communications", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 193-210, Springer-Verlag, 1993.

[1221] G.S. VERNAM, "Secret signaling system", U.S. Patent # 1,310,719, 22 Jul 1919.

[1222] ———, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", *Journal of the American Institute for Electrical Engineers, 55* (1926), 109-115.

[1223] J. VON NEUMANN, "Various techniques used in connection with random digits", *Applied Mathematics Series, U.S. National Bureau of Standards*, 12 (1951), 36-38.

[1224] J. VON ZUR GATHEN AND V. SHOUP, "Computing Frobenius maps and factoring polynomials", *Computational Complexity, 2* (1992), 187-224.

[1225] V.L. VOYDOCK AND S.T. KENT, "Security mechanisms in high-level network protocols", *Computing Surveys, 15* (1983), 135-171.

[1226] D. WACKERLY, W. MENDENHALL III, AND R. SCHEAFFER, *Mathematical Statistics with Applications*, Duxbury Press, Belmont, California, 5th edition, 1996.

[1227] M. WAIDNER AND B. PFITZMANN, "The dining cryptographers in the disco: Unconditional sender and recipient untraceability with computationally secure serviceability", *Advances in Cryptology-EUROCRYPT '89 (LNCS 434)*, *690*, 1990.

[1228] C.P. WALDVOGELAND J.L. MASSEY, "The probability distribution of the Diffie-Hellman key", *Advances in Cryptology-A USCRYPT* '92 *(LNCS 718)*, *492-504*, 1993.

Index

Symbols

$|S|$ (cardinality of a set S), 49
∈ (set member), 49
⊆ (subset), 49
c (proper subset), 49
∩ (set intersection), 49
∪ (set union), 49
− (set difference), 49
x (Cartesian product), 49
0 (empty set), 50
O-notation (big 0), 58
R-notation (big Omega), 59
Q-notation (big Theta), 59
o-notation (little-o), 59
$L_q[\alpha$, c] (subexponential notation), 60
$\leq_P$ (polytime reduction), 61
∼ (asymptotic equivalence), 134
π (mathematical constant pi), 49
e (base of natural logarithms), 49
$\sum$ (sum), 50
$\prod$ (product), 50
! (factorial), 50
$\lfloor\ \rfloor$ *(floor), 49*
$\lceil\ \rceil$ (ceiling), 49
ϕ (Euler phi function), 65,286
$\mu(n)$ (Mobius function), 154
lg (base 2 logarithm), 50
ln (natural logarithm), 50
| (divides relation), **63, 79**
≡ (congruence relation), **67, 79**
≪ (much less than), 529
≫ (much greater than), 170
$\binom{n}{k}$(binomial coefficient), 52
$\left(\frac{a}{p}\right)$(Legendre symbol), 72
< > (inner product), 118
$\|x\|$ (length of a vector x), 118
atb (assignment operator), 66
$a\|b$ (concatenation of strings *a,b*), *38*
$\{0,1\}^k$ (bitstrings of bitlength k), 447
$\{0,1\}^*$ (bitstrings of arbitrary bitlength), 447
$\mathbb{Q}$ (the rational numbers), 49
$\mathbb{R}$ (the real numbers), 49
$\mathbb{Z}$ (the integers), 49
$\mathbb{Z}_n$ (integers modulo n), 68
$\mathbb{Z}_n^*$ (multiplicative group of $\mathbb{Z}_n$), 69
Q_n (quadratic residues modulo n), 70
$\overline{Q}_n$ (quadratic non-residues modulo n), 70
$\mathbb{F}_q$ (finite field of order *q), 8 1*
$\mathbb{F}_q^*$ (multiplicative group of F,), 81
$R[x]$ (polynomial ring), 78
∨ (inclusive-OR), 213
⊕ (exclusive-OR), 20
A (AND), 213
❑ (addition mod 2^n), 263
El (subtraction mod 2^n), 270
⊙ (modified multiplication mod $2^n + 1$), 263
↩ (left rotation), 213
↪ (right rotation), 213
$A \rightarrow B$ (message transfer), 396

A

Abelian group, 75
Abstract Syntax Notation One (ASN. 1), 660
Access control, 3
Access control matrix, 387
Access matrix model, 569
Access structure, 526
- monotone, 527

Accredited Standards Committee (ASC), 648
Active adversary, **15, 37**
Active attack, 41,495
Ad hoc security, 43
Adaptive chosen-ciphertext attack, 42
Adaptive chosen-message attack, 433
Adaptive chosen-plaintext attack, 41
Addition chains, 621,633
Adversary, 13,495
- active, 15
- insider, 496
  - one-time, 496
  - permanent, 496
- outsider, 496
- passive, 15

Affine cipher, 239
Algebraic normal form, 205
Algorithm
- definition of, 57
- deterministic, 62
- exponential-time, 59

[1258] ———, "Theory and applications of trapdoor functions", *Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science*, 80-91, 1982.

[1259] S.-M. YEN AND C.-S. LAIH, "New digital signature scheme based on discrete logarithm", *Electronics Letters*, 29 (June 10, 1993), 1120-1121.

[1260] C. YUEN, "Testing random number generators by Walsh transform", *IEEE Transactions on Computers*, *26* (1977), 329-333.

[1261] D. YUN, "Fast algorithm for rational function integration", *Information Processing 77: Proceedings of IFIP Congress 77*, 493–498, 1977.

[1262] G. YUVAL, "How to swindle Rabin", *Cryptologiu*, *3* (1979), 187–190.

[1263] K. ZENG AND M. HUANG, "On the linear syndrome method in cryptanalysis", *Advances in Cryptology-CRYPTO '88 (LNCS 403)*, 469-478, 1990.

[1264] K. ZENG, C.-H. YANG, AND T.R.N. RAO, "On the linear consistency test (LCT) in cryptanalysis with applications", *Advances in Cryptology-CRYPTO '89 (LNCS 435)*, 164-174, 1990.

[1265] ———, "An improved linear syndrome algorithm in cryptanalysis with applications", *Advances in Cryptology-CRYPTO '90 (LNCS 537)*, 34-47, 1991.

[1266] K. ZENG, C.-H. YANG, D.-Y WEI, AND T.R.N. RAO, "Pseudorandom bit generators in stream-cipher cryptography", *Computer*, 24 (1991), 8-17.

[1267] C. ZHANG, "An improved binary algorithm for RSA", *Computers and Mathematics with Applications*, 25:6 (1993), 15-24.

[1268] Y. ZHENG, J. PIEPRZYK, AND J. SEBERRY, "HAVAL – a one-way hashing algorithm with variable length of output", *Advances in Cryptology-AUSCRYPT '92 (LNCS 718)*, 83–104, 1993.

[1269] Y. ZHENG AND J. SEBERRY, "Immunizing public key cryptosystems against chosen ciphertext attacks", *IEEE Journal on Selected Areas in Communications*, 11 (1993), 715-724.

[1270] N. ZIERLER, "Primitive trinomials whose degree is a Mersenne exponent", *Information and Control*, 15 (1969), 67-69.

[1271] N. ZIERLER AND J. BRILLHART, "On primitive trinomials (mod 2)", *Information and Control*, 13 (1968), 541-554.

[1272] P.R. ZIMMERMANN, *The Official PGP User's Guide*, MIT Press, Cambridge, Massachusetts, 1995 (second printing).

[1273] J. ZIV AND A. LEMPEL, "On the complexity of finite sequences", *IEEE Transactions on Information Theory*, *22* (1976), 75-8 1.

[1274] M. ŽIVKOVIĆ, "An algorithm for the initial state reconstruction of the clock-controlled shift register", *IEEE Transactions on Information Theory*, *37* (1991), 1488-1490.

[1275] ———, "A table of primitive binary polynomials", *Mathematics of Computation*, *62* (1994), 385-386.

[1276] ——— "Table of primitive binary polynomials. 'II", *Mathematics of Computation*, *63* (1994), 301-306.

Base *b* representation, 592
Bayes' theorem, 51
BEAR block cipher, 282
Beaufort cipher, 241
Beller-Yacobi key transport
  2-pass, 5 14
  4-pass, 5 13
Berlekamp's Q-matrix algorithm, 124, 132
Berlekamp-Massey algorithm, 200-201
  next discrepancy, 200
Bernoulli trial, 52
Big-endian, 344
Big-O notation, 58
Bijection, 7
Binary additive stream cipher, 194
  keystream generator, 194
  running key generator, 194
Binary alphabet, 11
Binary Euclidean algorithm, 632
Binary extended gcd algorithm, **608–610, 632**
Binary gcd algorithm, **606–607, 632**
Binary operation, 75
Binary representation, 592
Binary tree, 557
  balanced, 558
  children, 557
  depth of, 558
  internal vertex, 557
  leaf, 557
  parent, 557
  root vertex, 557
Binomial
  coefficient, 52
  distribution, 52
  theorem, 52
Biometrics, 387,420
Birthday attack, 352,369
Birthday problem, 53
Birthday surprise, 53
Bit commitment, 421
Bitzer's hash function, 374
Black-box, **329, 341, 369, 378**
Blakley's threshold scheme, 538
Blind signature scheme, 475,487
  based on DSA, 487
  based on Nyberg-Rueppel, 487
  Chaum, 475
  fair, 487
Blinded message, 475
Blinding function, 475
  based on RSA, 475
Blob, 421
Block cipher, 223-282
  3-WAY, 28 1
  attacks on
    differential cryptanalysis, 258
    differential-linear, 271
    exhaustive key search, 233-234,273
    key clustering attack, 28 1
    linear cryptanalysis, 258
    meet-in-the-middle attack, 235
    related-key attack, 226, 281
    time-memory tradeoff, 236,273
    truncated differentials, 27 1,280
  BEAR, 282
  Blowfish, 281
  CAST, 28 1
  classical cipher, 237-250
  definition of, 16,224
  DES, 250-259
  double DES, 235
  FEAL, 259-262
  GOST, 282
  IDEA, 263-265
  iterated, 25 1
  Khafre, 271
  Khufu, 27 1
  LION, 282
  LOKI'9 1,270
  Luby-Rackoff, 282
  Lucifer, 276
  modes of operation, 228-233, 272
    ANSI X3.106 standard, 649
    ANSI X9.52 standard, 65 1
    CBC with checksum (CBCC), 367
    cipher feedback mode (CFB), 23 1
    cipher-block chaining mode (CBC), 230
    counter mode, 233
    electronic codebook mode (ECB), 228-*230*
    FIPS 8 1 standard, 654
    IS0 8372 standard, 645
    ISO/IEC 10116 standard, 647
    output feedback mode (OFB), 232-233
    plaintext-ciphertext block chaining (PCBC), 368
  Randomized DES (RDES), 278
  RC2, 282
  RC5, 269–270
  round function, 25 1
  SAFER, 266-269
  semi-weak keys (of DES), 257
    anti-palindromic keys (of DES), 257
  SHARK, 281
  SKIPJACK, 282,584
  TEA, 282
  triple DES, 272
  WAKE. 282

polynomial-time, 59
randomized, 62
expected running time, 63
running time, 58
asymptotic, 58
average-case, 58
worst-case, 58
subexponential-time, 60
Alphabet of definition, 11
Alternating step generator, 209-211, 220
Anonymity, 3
ANSI standards, 648-65 1,660
ordering and acquiring, 656
ANSI X9.17 pseudorandom bit generator, 173
Anti-palindromic keys of DES, 257
Appended authenticator, 361
Arbitrated signature scheme, 472-473
Arithmetic
integer, see Multiple-precision integer arithmetic
modular, see Multiple-precision modular arithmetic
Arthur-Merlin games, 421
ASN. 1, see Abstract Syntax Notation One (ASN.l)
Asymmetric cryptographic system, 544
Asymptotic running time, 58
Atkin's primality test, 145
implementation report, 166
Attack
active, 41,495
adaptive chosen-ciphertext, 42
adaptive chosen-message, 433
adaptive chosen-plaintext, 41
chosen-ciphertext, 41,226
chosen-message, 433
chosen-plaintext, 41,226
chosen-text, 417
ciphertext-only, 41,225
dictionary, 42,392
differential cryptanalysis, 258
differential-linear, 271
exhaustive key search, 233-234
forced delay, 417
forward search, 42,420
impersonation, 42,417
interleaving, **42, 417, 531,** 540
intruder-in-the-middle, 530, 540
key-only, 432
known-key, **42, 496, 534**
known-key triangle, 538
known-message, 432
known-plaintext, 41,225
linear cryptanalysis, 258
local, 419
meet-in-the-middle, 235
misplaced trust in server, 53 1
non-interactive, 419
off-line, 419
on-line, 419
passive, 41,495
pre-play, 397
reflection, **417, 530, 540**
related-key, 226
remote, 419
replay, 42,417
time-memory tradeoff, 236
truncated differentials, 271
universal forgery, 482
Attacker, 13
Attacker (alternate names), 495
see *also* Adversary
Attribute certificate, 561
Audit trail information, 545
Authenticated key establishment, 492,493
Authenticated key exchange protocol
AKEP1/AKEP2, 499, 535, 541
Authentication
data origin, 4,361
see *also* Data origin authentication
entity, 4
see *also* Entity authentication
explicit key, 492
key, 492
message, 361
mutual, 494
protocol, 493
transaction, 362
unilateral, 494
see *also* Entity authentication (and Identification)
Authentication code, 376,382
Authentication path, 557
Authentication server, 491,549
Authentication tree, **466–468, 485, 556–559,** 587
Authority revocation list **(ARL),** 577
Authorization, 3
Authorized subset, 527
Auto-key cipher, 242
Autocorrelation function, 180
Autocorrelation test, 182
Auxiliary-input zero-knowledge, 423
Avalanche effect, 277
Average-case running time, 58

B
Baby-step giant-step algorithm, 104-106, 128
BAN logic, **420, 534, 541**
Bandwidth efficiency, 437
Barrett reduction, **603–605, 631**

mean of, 177
variance of, 177
Chinese remainder theorem, 68
Gamer's algorithm, 612-613
Gauss's algorithm, 68
Chipcard, 387,424
Chor-Rivest public-key encryption, 302-306, 318
attacks on, 3 18
decryption algorithm, 303
encryption algorithm, 303
key generation, 303
recommended parameter sizes, 305
security of, 305
Chosen-ciphertext attack, 41,226, 285
adaptive, 285
indifferent, 285
Chosen-message attack, 433
directed, 482
generic, 482
Chosen-plaintext attack, 41, 226
Cipher, 12
see *also* Encryption
Cipher-block chaining mode (CBC), 230
integrity of IV in, 230
use in public-key encryption, 285
Cipher feedback mode (CFB), 231
as a stream cipher, 233
IS0 variant of, 23 1
Cipher machine, 242-245
Jefferson cylinder, 243
rotor-based machine, 243-245, 276
Enigma, 245
Hagelin M-209,245
Hebem, 244
Wheatstone disc, 274
Ciphertext, 11
Ciphertext-only attack, 41,225
Ciphertext space, 11
Claimant, 385, 386
Classical cipher, 237-250, 273-276
cipher machines, see Cipher machine
cryptanalysis, **245–250**, 275-276
index of coincidence, 248
Kasiski's method, 248
measure of roughness, 249
polyalphabetic substitution cipher, see Polyalphabetic substitution cipher
substitution cipher, see Substitution cipher
transposition cipher, see Transposition cipher
Classical modular multiplication, 600
Classical occupancy problem, 53
Claw-resistant (claw-free), 376,468
Clipper chip, 584,589
key escrow, 584
law enforcement access field (LEAF), 584
Clipper key escrow, 654
Clock-controlled generator, 209-2 12
Codebook, 240
Codomain of a function, 6
Collision, 321
pseudo-collision, 371
Collision resistance, 324, 325
Collision resistant hash function (CRHF), 325
Combining function, 205
Common modulus attack on RSA, 289
Commutative ring, 77
Complementation property of DES, 256-257
Complete function, 277
Complexity classes, 59-62
BPP, 63
co-NP, 60
NP, 60
NP-complete, 61
NP-hard, 62
NPC, 61
P, 60
RP, 63
ZPP, 63
Complexity measure
2-adic span, 2 18
linear complexity, 198-201
maximum order complexity, 217
Turing-Kolmogorov-Chaitin complexity, 217
Ziv-Lempel complexity, 217
Complexity of attacks on a block cipher, 225-227
active complexity, 226
attack complexity, 226
data complexity, 226
passive complexity, 226
processing complexity, 226
storage complexity, 226
Complexity theory, 57-63
Complexity-theoretic security, 43
Compliant, 532
Composite integer, 64
Composition of functions, 19
Computation-resistance (MAC), 325
Computational problems
computationally equivalent, 88
polytime reduction, 88
Computational security, 43,226
Computational zero-knowledge protocol, 407
Computationally equivalent decision problems, 61
COMSET, 421,536
Conditional entropy, 56
Conditional probability, 5 1
Conditional transinformation, 57
Conference keying, 528-529, 540

Block of a sequence, 180
Blocklength, 224
Blom's KDS bound, 505
Blom's key pre-distribution system, 506, 536
Blowfish block cipher, 281
Blum integer, 74-75
Blum-Blum-Shub pseudorandom bit generator, 186-187,308
Blum-Goldwasser probabilistic public-key encryption, 308-3 11
decryption algorithm, 309
encryption algorithm, 309
key generation, 308
security of, 3 10
Blum-Micali pseudorandom generator, 189
Blundo's conference KDS bound, 529
Boolean function, 202
algebraic normal form of, 205
correlation immune, 207
nonlinear order of, 205
Break-backward protection, 496
Brickell-McCurley identification protocol, 423
Broadcast encryption, 528
Bucket hashing, 382
Burmester-Desmedt conference keying, 528
Burst error, 363

C

CA, see Certification authority (CA)
Caesar cipher, 239
CALEA, 590
Capstone chip, 589
Cardinality of a set, 49
Carmichael number, 137
Carry-save adder, 630
Cartesian product, 49
Cascade cipher, 234, 237
Cascade generator
m-sequence, 221
p-cycle, 220
Cascading hash functions, 334
CAST block cipher, 281
patent, 659
CBC, see Cipher-block chaining mode
CBC-MAC, 353-354,367
ANSI X9.9 standard, 650
ANSI X9.19 standard, 650
FIPS 113 standard, 654
IS0 8731-1 standard, 652
IS0 9807 standard, 652
ISO/IEC 9797 standard, 646
Cellular automata stream cipher, 222
Certificate
ANSI X9.45 standard, 65 1
ANSI X9.55 standard, 65 1
ANSI X9.57 standard, 65 1
caching, 576
chain, 572
directory, 549
pull model, 576
push model, 576
forward, 575
on-line, 576
reverse, 575
revocation, 566, 576–577
RFC 1422,655
secret-key, see Secret-key certificate
symmetric-key, see Symmetric-key certificate
X.509 standard, 660
Certificate of primality, 166
Certificate revocation list (CRL), 576-577
Certification, 3
path, 572
policy, 576
topology, 572
Certification authority (CA), 491,548, 556,559
Certificational attack, 236
Certificational weakness, 285
CFB, see Cipher feedback mode
CFB-64 MAC, 650
Challenge, 397,409
Challenge-response identification, 397-405, 420-421
public-key, 403–405
ISOAEC 9798-3, 404–405
modified Needham-Schroeder, 404
x.509,404
symmetric-key, 400-403
ISO/IEC 9798-2, 401–402
SKID2, 402
SKID3, 402
Channel, 13
physically secure, 13
secure, 13
secured, 13
unsecured, 13
Characteristic of a field, 77
Chaum's blind signature protocol, 475
Chaum-van Antwerpen undeniable signature scheme, 476-478
disavowal protocol, 477
key generation, 476
security of, 478
signature generation, 476
Chebyshev's inequality, 52
Checksum, 362, 367–368
Chi-square (χ^2) distribution, 177-179
degrees of freedom, 177

  test vectors, 256
  triple-DES, 273
  weak key, 257
    fixed point of, 257
Designated confirmer signature, 487
Deterministic algorithm, 62
Dickson polynomial, 3 14
Dickson scheme, 3 14
Dictionary attack, 42
Difference of sets, 49
Differential chaining attack, 375
Differential cryptanalysis
  of block ciphers, 258, **271, 278–280**
Differential-linear cryptanalysis, 271
Diffie-Hellman key agreement, **515–520, 522–524**
  ANSI X9.42 standard, 651
  composite modulus, 537
  patent, 637
Diffie-Hellman problem, 113-I 14
  composite moduli, 114, 131
  generalized, 113
Diffie-Lamport one-time signature scheme, 485
Diffusion, 20
Digital fingerprint, 321
Digital signature, see Signature
Digital Signature Algorithm (DSA), 452454,483
  ANSI X9.30- 1 standard, 65 1
  FIPS 186 standard, 655
  key generation, 452
  patent, 640,658
  security of, 453
  signature generation, 452
  signature verification, 453
  use and throw coupons, 483
Dimension of a vector space, 80
Dirichlet theorem, 135
Disavowal protocol, 477
Discrete Fourier Transform **(DFT),** 63 1
Discrete logarithms, 103-113
  baby-step giant-step algorithm, 104-106
  composite moduli, 114
  exhaustive search, 104
  for class groups, 130
  for elliptic curves, 130
  for hyperelliptic curves, 130
  function field sieve, 129
  generalized problem, 103
  heuristic running time, 129
  in subgroups of $\mathbb{Z}_p^*$, 113
  index-calculus algorithms, 109-112
  lambda method, 128
  number field sieve, 128
  Pohlig-Hellman algorithm, 107-109
  Pollard's rho algorithm, 106-107
  problem definition, 103
  rigorously analyzed algorithms, 129
  security of individual bits, 116
Division
  of integers, 63
  of polynomials, 79
Division algorithm
  for integers, 64
  for polynomials, 78
Dixon's algorithm, 95, 127
DNA computer, 130
Domain of a function, 6
Double DES, 235
Double-length MDC, 339
DSA, see Digital Signature Algorithm
Dynamic key establishment, 491
Dynamic secret sharing scheme, 527

E

E-D-E triple encryption, 235, 272
E-E-E triple encryption, 272
Eavesdropper, 13,495
ECB, see Electronic **codebook** mode
Effective key size, 224
Electronic cash
  divisible, 487
  untraceable, 487
Electronic **codebook** mode (ECB), 228-230
ElGamal key agreement, 5 17
ElGamal public-key encryption, **294–298**
  generalized
    decryption algorithm, 297
    encryption algorithm, 297
    key generation, 297
  in $\mathbb{Z}_p^*$
    decryption algorithm, 295
    encryption algorithm, 295
    key generation, 294
    recommended parameter sizes, 296
  security of, 296
ElGamal signature scheme, **454–459, 484**
  generalized
    key generation, 458
    signature generation, 458
    signature verification, 458
  in $\mathbb{Z}_p^*$
    key generation, 454
    security of, **455–456**
    signature generation, 454
    signature verification, 454
  signature verification, 618
  variants of, 457
Elliptic curve
  discrete logarithm problem, 130

Blundo's conference KDS bound, 529
Burrnester-Desmedt, 528
definition of, 528
Confidentiality, **3, 4,** 12
Confirmation, 3
Confounder, 418
Confusion, 20
Congruences
integers, 67
polynomials, 79
Conjugate gradient method, 129
Connection polynomial of an LFSR, 196,204
known versus secret, 204
sparse versus dense, 205
Constrained linear equations problem, 423
Continued fraction factoring algorithm, 126
Continuous random variable, 176
Control vector, 569
patent, 639, 658
Conventional encryption, 15
Correcting-block chaining attack, 373
Correlation attack, 206,218
Correlation immunity, 207, 218
Counter mode, 233
CRC-based MAC, 359
Credential, 501
Cross-certificate (CA-certificate), 572
Cross-certificate pair, 573
Cryptanalysis, 15
Cryptanalyst, 15
Cryptographic check value, 363
Cryptographic primitives, 4
taxonomy of, 5
Cryptographically secure pseudorandom bit generator (CSPRBG), 185-187
Blum-Blum-Shub generator, 186-l 87
Blum-Micali generator, 189
definition of, 171
Micah-Schnorr generator, 186
modified-Rabin generator, 190
RSA generator, 185-l 86
Cryptography
definition of, 4
goals of, 4
CRYPTOKI, 656
Cryptology, 15
Cryptoperiod of a key, 553
Cryptosystem, 15
Cut-and-choose protocol, 410,421
Cycle of a periodic sequence, 180
Cyclic group, **69, 76**
generator of, 76
Cyclic redundancy code (CRC), 363
Cyclic register, 220
Cycling attacks on RSA, **289, 3** 13

D
Data Authentication Algorithm (DAA), 654
Data Encryption Standard, see DES block cipher
Data integrity, **3, 4, 33, 359–368,** 383
Data key, 552
Data origin authentication, **3, 4, 25,** 359-368,491
Davies-Meyer hash function, 341
de Bruijn FSR, 203
de Bruijn sequence, 203
De-skewing, 172
DEA, 649
Decimated subsequence, 211
Decision problems, 60
computationally equivalent, 61
polytime reduction, 61
Decryption, 11
Decryption exponent for RSA, 286
Decryption function, 11
DECT, 586
Degrees of freedom, 177
Delay element
of an FSR, 202
of an LFSR, 195
Delayed-carry adder, 630
Density of a knapsack set, 120
Derivative of a polynomial, 123
DES block cipher, **250–259, 276–278**
ANSI X3.92 standard, 649
attacks on
differential cryptanalysis, 258-259
exhaustive key search, 233-234,272
linear cryptanalysis, 258-259
complementation property, 256-257
decryption algorithm, 255
DESX, 273
double DES, see Double DES
encryption algorithm, 253
expansion permutation, 252
FIPS 46 standard, 654
initial permutation (IP), 252,277
key schedule
decryption, 256
encryption, 255
modes of operation, see Block cipher, modes of operation
patent, 636
permuted choices **(PC1, PC2),** 252
properties and strengths, 256-259
round, 252
S-box, 252
semi-weak key, 257
anti-fixed point of, 257

feedback bit of, 202
feedback function of, 202
Feedback with carry shift register (FCSR), 217-218,222
initial state of, 202
linear feedback shift register, see Linear feedback shift register (LFSR)
non-singular, 203
nonlinear feedback shift register, 202
output sequence of, 202
stage of, 202
Feedback with carry shift register (FCSR), 217-218, 222
Feige-Fiat-Shamir identification protocol, **410–412**, 422
Feige-Fiat-Shamir signature scheme, **447–449, 483**
identity-based modification, 449
key generation, 447
security of, 448
signature generation, 448
signature verification, 448
Feistel cipher, 25 1, 276
Fermat liar, 136
Fermat number, 143, 166
Fermat witness, 136
Fermat's primality test, 136
Fermat's theorem, 69
Fiat-Shamir identification protocol
basic version, 408
patent, 638, 658
Fiat-Shamir signature scheme, 483
patent, 638, 658
Field, 77
characteristic of, 77
definition of, 77
extension field of, 77
finite, see Finite field
subfield of, 77
Filtering function, 208
Finite field, 80-85
definition of, 80
order of, 80
polynomial basis, 83
FIPS, **654–655, 661**
ordering and acquiring, 656
FIPS 186 pseudorandom bit generator, 174-175
FISH stream cipher, 222
Fixed-point chaining attack, 374
Floyd's cycle-finding algorithm, 91, 125
Forced delay attack, 417
Formal methods, 534,541
Forward certificate, 575
Forward error correction, 363
Forward search attack, **34, 42, 420**
Fractionation, 276
Frequency distribution
of English **digrams**, 247
of single English characters, 247
Frequency test, 18 1
Fresh key, 494
Function, 6-10
bijection, 7
composition of, 19
definition of, 6
injective, 46
inverse, 7
involution, 10
one-to-one, 7
one-way, 8
onto, 7
permutation, 10
surjective, 46
trapdoor one-way, 9
Function field sieve, 129
Functional diagram, 6
Functional graph, 54
component size, 55
cycle length, 55
predecessors size, 55
rho-length, 55
tail length, 55
tree size, 55
Functionally trusted third party, 39

G
Gap of a sequence, 180
Gamer's algorithm, 612-613
Gauss's algorithm, 68
Gaussian integer method, 128
gcd, see Greatest common divisor
Geffe generator, 206
General-purpose factoring algorithm, 90
Generator
of a cyclic group, 76, 160
algorithm for finding, 163
of $\mathbb{F}_{2^m}^*$, 163
of $\mathbb{Z}_n^*$, 69
of $\mathbb{Z}_p^*$, 164
algorithm for selecting, 164
Generator matrix, 506
Girault self-certified public key, 522
GMR one-time signature scheme, 468-471, 486
authentication tree, 470
key generation, 469
security of, 470
signature generation, 469
signature verification, 469
GOAL stream cipher, 219

ElGamal public-key encryption, 297
in public-key cryptography, 316
patents, 659
RSA analogue, 3 15
supersingular curve, 3 16
Elliptic curve factoring algorithm, 94, 125
implementation reports, 126
Elliptic curve primality proving algorithm, 145
Encrypted key exchange (EKE), 538
Encryption, 11
see *also* Block cipher
see *also* Public-key encryption
see *also* Stream cipher
Encryption exponent for RSA, 286
Encryption function, 11
Encryption scheme, 12
breakable, 14
Enemy, 13,495
Enigma, 245, 276
Entity, 13
Entity authentication, 3, 386,491
ANSI X9.26 standard, 651
FIPS JJJ standard, 655
ISO 11131 standard, 652
ISO/IEC 9798 standard, **401–402, 404–405, 421,** 647
see *also* Identification
Entropy, 56-57, 246
Ephemeral secret, 494
Equivocation, 56
Error-correcting code, 363
Escrowed Encryption Standard (EES)
FIPS 185,654
ESIGN signature scheme, 473474,486
key generation, 473
patent, 638, 658
security of, 474
signature generation, 473
signature verification, 473
Euclidean algorithm
for integers, 66
for polynomials, 81-83
Euler liar, 138
Euler phi function (ϕ), 65
Euler pseudoprime, 138
Euler witness, 137
Euler's criterion, 137
Euler's theorem, 69
Exclusive-or (XOR), 20
Exhaustive key search, **14, 233–234, 272**
Existential forgery, 30,432
exp (exponential function), 50
Expected running time, 63
Explicit authentication, 492
Exponent array, 617
Exponent recoding, see Exponentiation
Exponential-time algorithm, 59
Exponentiation, 613-629, 633-634
addition chains, 621
exponent recoding, 627-629
signed-digit representation, 627-628
string-replacement representation, 628-629
fixed-base comb method, 625-627
fixed-base Euclidean method, 624-625
fixed-base windowing method, 623-624
left-to-right binary method, 615
left-to-right k-ary method, 615
modified left-to-right k-ary method, 616
Montgomery method, 619-620
repeated square-and-multiply algorithm, 71, 84
right-to-left binary method, 614
simultaneous multiple, 617-618
sliding-window method, 616
vector-addition chains, 622-623
Extendable secret sharing scheme, 526
Extended Euclidean algorithm
for integers, 67
for polynomials, 82
Extended Riemann Hypothesis (ERH), 165
Extension field, 77
Extractor, 406

F

Factor base, 94, 109
Factoring integers, see Integer factorization
Factoring polynomials, see Polynomial factorization
Fail-stop signature scheme, **478–481, 488**
Heyst-Pedersen, 478-48 1
Fair blind signature scheme, 487
Fair cryptosystems, 640-641, 658
for Diffie-Hellman key agreement, 641
patent, 640
FEAL block cipher, **259–262, 278–279**
attacks on, 278-279
FEAL decryption algorithm, 261
FEAL-8 encryption algorithm, 261
FEAL-8 key schedule, 261
FEAL-N, 262
FEAL-NX, 262
patent, 639
test vectors, 262
Feedback shift register (FSR), 195-203
de **Bruijn,** 203
definition of, 202
delay element of, 202

  - key generation, 478
  - proof-of-forgery algorithm, 481
  - signature generation, 479
  - signature verification, 479
- High-order digit, 593
- Hill cipher, 240,274
- Historical work factor, 44
- HMAC, 355
- Homomorphic property of RSA, 289
- Homophonic substitution cipher, 17,240
- Hybrid protocol, 5 12
- Hyperelliptic curve
  - discrete logarithm problem, 130
  - ElGamal public-key encryption, 297
- Hypothesis testing, 179-l 80

I

- IC card, 387
- IDEA block cipher, **263–265**, **279–280**
  - attacks on, 279-280
  - decryption algorithm, 264
  - encryption algorithm, 264
  - key schedule, 264
  - patent, 640, 658
  - test vectors, 265
  - weak keys, 279
- Ideal secret sharing scheme, 526,527
- Identification, **3**, **24–25**, **385–424**
  - applications of, 387
  - attacks on, **417–420**, **424**
    - chosen-text, 417
    - forced delay, 417
    - impersonation, 417
    - interleaving, 417
    - local, 419
    - non-interactive, 419
    - off-line, 419
    - pre-play, 397, 398
    - reflection, 417
    - remote, 419
    - replay, 417
  - challenge-response, see Challenge-response identification
  - mutual, 387
  - passwords, see Passwords (weak authentication)
  - questionnaire-based, 420
  - relation to signatures, 388
  - unilateral, 387
  - zero-knowledge, see Zero-knowledge identification
  - see *also* Entity authentication
- Identification Friend or Foe **(IFF)** system, 421
- Identity verification, 385
- Identity-based key establishment, 493
- Identity-based system, 538, 561-562, 587
- IEEE **P1363** standard, 660
- **IETF**, 655
- Image of a function, 6
- Impersonation, **27**, **42**, 386,417
- Impersonator, 495
- Implicit key authentication, see Key authentication
- Implicitly-certified public key, **520–522**, **562–563**, *588*
  - Diffie-Hellman using, 522-524
  - identity-based, 563
  - of Girault, 522
  - of Gunther, 521
  - self-certified, 563
- Imprint, 321
- Improved PES (IPES), 279
- In-line trusted third party, 547
- Incremental hashing, 378
- Independent events, 5 1
- Index of coincidence, 248,275
- Index-calculus algorithm, 109-112, 128
  - Gaussian integer method, 128
  - in $\mathbb{F}_{2^m}$, 111
    - implementation reports, 128
  - in $\mathbb{Z}_p$, 110
    - implementation reports, 128
  - linear sieve, 128
  - residue list sieve, 128
- Information dispersal algorithm (IDA), 539
- Information rate, 527
- Information security, 2
  - objectives of, 3
- Information security service, 14
  - breaking of, 15
- Information theory, 56-57
- Initial state
  - of an FSR, 202
  - of an LFSR, 196
- Injective function, 46
- Inner product, 118
- Input size, 58
- Insider, 496
  - one-time, 496
  - permanent, 496
- Integer
  - multiple-precision, 593
  - negative
    - signed-magnitude representation, 593
    - two's complement representation, 594
  - single-precision, 593
- Integer arithmetic, see Multiple-precision integer arithmetic
- Integer factorization, 89-98
  - continued fraction algorithm, 126

Goldwasser-Kilian primality test, 166
Goldwasser-Micali probabilistic public-key encryption, 307-308
  decryption algorithm, 307
  encryption algorithm, 307
  key generation, 307
  security of, 308
Golomb's randomness postulates, 180
Goppa code, **299, 3** 17
Gordon's algorithm for strong prime generation, 150
GOST block cipher, 282
GQ identification protocol, **412–414, 422**
  patent, 639, 658
GQ signature scheme, **450–45** 1
  key generation, 450
  message recovery variant, 45 1
  patent, 639, 658
  security of, 45 1
  signature generation, 450
  signature verification, 450
Grandmaster postal-chess problem, 418
Greatest common divisor
  binary extended gcd algorithm, **608–610, 632**
  binary gcd algorithm, 606-607, 632
  Euclidean algorithm, 66
  Lehmer's gcd algorithm, **607–608, 632**
  of integers, 64
  of polynomials, 81
Group, 75-76
  cyclic, 76
  definition of, 75
  order of, 75
  subgroup of, 76
Group signature, 488
GSM, 586
GSS-API, 655,661
Gunther's implicitly-certified public key, 521
Gunther's key agreement, 522

H

Hagelin M-209,245,276
Hamming weight, 105
Handwritten signature, 23
Hard predicate, 115
Hash function, 33, 321-383
  alternate terminology, 325, 371
  applications, 321-322, 330-331
  attacks, 368-375
    birthday, 369-371
    chaining, 373-375
    Pseudo-collisions, 371-373
  based on block ciphers, 338-343
    Abreast Davies-Meyer, 380
    Davies-Meyer, 341
    Matyas-Meyer-Oseas, 341
    MDC-2,342
    MDC-4,343
    Merkle's DES-based hash, **338, 339, 378**
    Miyaguchi-Preneel, 341
    N-Hash, 380
    Tandem Davies-Meyer, 380
  based on modular arithmetic, 351-352
    MASH-l, 352
    MASH-2,352
  cascading, 334
  collision resistant (CRHF), 325
  customized, 343-351
    HAVAL, 379
    MD2, 380
    MD4, 346
    MD5, 347
    RIPEMD, 380
    RIPEMD-128, 339, 380
    RIPEMD-160, 339, 350
    Secure Hash Algorithm (SHA-l), 348
    Snefru, 380
  definition of, 322
  ideal security, 336
  initialization value (IV), 335
  MD-strengthening, see MD-strengthening
  Merkle's meta-method, 333
  one-way (OWHF), 325
  padding, 334-335
  properties of
    2nd-preimage resistance, 323
    collision resistance, 324
    compression, 322
    ease of computation, 322
    local one-wayness, 331
    near-collision resistance, 331
    non-correlation, 33 1
    partial-preimage resistance, 331
    preimage resistance, 323
    strong collision resistance, 324
    weak collision resistance, 324
  r-collision resistant, 424
  strong one-way, 325
  universal classes of, 376
  universal one-way, 377
  weak one-way, 325
Hash-code, 321
Hash-result, 321
Hash-value, 33,321
HAVAL hash function, 379
Hellman-Merkle patent, 637,658
Heuristic security, 43,533
Heyst-Pedersen fail-stop signature scheme, 478-481

Key confirmation, 492
Key control, 494
Key derivation, 490,498
Key distribution
  confidential keys, 551-555
    key layering, 551-553
    key translation center, 553-554
    symmetric-key certificates, 554–555
  public keys, 555-566
    authentication trees, 556-559
    certificates, 559-561
    identity-based, 561-562
    implicitly-certified, 562-563
Key distribution center (KDC), 491, 500,547
Key distribution pattern, 536
Key distribution problem, 16, 546
Key distribution system (KDS), 505
  Blom's KDS bound, 505
  security against coalitions, 505
Key escrow, 584-586
  agent, 550,584
  Clipper, 584
Key establishment, 489-541
  analysis of, 530-534, 540-541
  attacks on
    interleaving, 53 1
    intruder-in-the-middle, 530
    misplaced trust in server, 531
    reflection, 530
  authenticated, 492,493
  compliant, 532
  definition of, 35,490
  identity-based, 493
  key agreement, see Key agreement
  key transport, see Key transport
  message-independent, 493
  operational, 532
  resilient, 532
  simplified classification, 491
Key life cycle, 577-581
  key states, 580
Key management, 36–38, 543–590
  ANSI X9.17 standard, 650
  ANSI X9.24 standard, 650
  ANSI X9.28 standard, 651
  ANSI X9.42 standard, 65 1
  centralized, 546
  controlling key usage, 567-570
  definition of, 35,544
  IS0 8732 standard, 652
  IS0 10202-7 standard, 652
  ISO 11166 standard, 652
  IS0 11568 standard, 653
  ISO/IEC 11770 standard, 647
  key agreement, see Key agreement
  key distribution, see Key distribution
  key establishment, see Key establishment
  key life cycle, 577-581
  key transport, see Key transport
Key management facility, 549
Key notarization, 568
  patent, 642,658
Key pair, 12
Key pre-distribution scheme, 540
  definition of, 490
Key server, 549
Key space, 11, 21, 224
Key tag, 568
Key translation center (KTC), 491, 500, 547, 553
Key transport, 35, 497–504, 506–515, 535–536
  AKEP1, 499
  AKEP2, 499
  Beller-Yacobi (2-pass), 514
  Beller-Yacobi (4-pass), 5 13
  COMSET, 536
  definition of, 490
  Kerberos, 501-502
  Needham-Schroeder public-key, 508
  Needham-Schroeder shared-key, 503
  Otway-Rees protocol, 504
  relation to key agreement, 491
  Shamir's no-key protocol, 500
  X.509 three-way, 512
  X.509 two-way, 5 11
Key update, 490
Keyed hash function, see Message authentication code (MAC)
Keying material, 544
Keying relationship, 544
Keystream, 20, 193, 194
Keystream generator, 21, 194
Khafre block cipher, 27 1
  attacks on, 281
  patent, 644
Khufu block cipher, 27 1
  attacks on, 281
  patent, 644
Knapsack generator, 209,220
Knapsack problem, 13 1
Knapsack public-key encryption, 300-306
  Chor-Rivest, 302-306
  Merkle Hellman, 300-302
Knapsack set, 117
  density of, 120
Known-key attack, 42,496, 534
Known-key triangle attack, 538
Known-message attack, 432
Known-plaintext attack, 41,225

Dixon's algorithm, 95, 127
elliptic curve algorithm, 94
general number field sieve, 98
general-purpose algorithms, 90
heuristic running times, 127
multiple polynomial quadratic sieve, 97
Pollard's $p-1$ algorithm, 92-93
Pollard's rho algorithm, 91-92
problem definition, 89
quadratic sieve algorithm, 95-97
random square methods, 94-98
special number field sieve, 98
special-purpose algorithms, 90
trial division, 90-91
Integers modulo n, 67-71
Integrity check value (ICV), 363
Interactive proof system, 406
Arthur-Merlin games, 421
completeness, 406
soundness, 406
Interleaving attack, 42,417, 53 1,540
Interloper, 13
Internal vertex, 557
Internet security standards, 655-656, 661
Intersection of sets, 49
Intruder, 13,495
Intruder-in-the-middle attack, 530, 540
Inverse function, 7
Inversion attack on stream ciphers, 219
Involution, 10
Irreducible polynomial, 78, **154–160**
algorithm for generating, 156
algorithm for testing, 155
number of, 155
primitive polynomial, see Primitivepolynomial
trinomials, 157
ISO standards, see ISO/IEC standards
ISO/IEC 9796, **442–444**, **482–483**
ISO/IEC standards, **645–648**, **651–653**, **660–661**
committee draft (CD), 645
draft international standard (DIS), 645
ordering and acquiring, 656
working draft (WD), 645
Iterated block cipher, 25 1
ITU, *653*

J

Jacobi sum primality test, 144, 166
Jacobi symbol, 73
computing, 73
Jefferson cylinder, 243, 274
Joint entropy, 56
JTC1, 645

K

Karatsuba-Ofman multiplication, 630
Kasiski's method, 248, 275
KDC, see Key distribution center (KDC)
Kerberos authentication protocol, **401**, **501–502**, *535-536*
RFC 1510,656
Kerckhoffs' assumption, 225
Kerckhoffs' desiderata, 14
Key, 11
archival, 580
backup, 580
cryptoperiod of, 553
data, 552
de-registration, 580
derived, 568
destruction, 580
fresh, 494
generator, 549
installation, 579
key-encrypting, 552
key-transport, 552
layering, 55 l-553
long-term, 553
master, 55 1
notarization, 568
offsetting, 568
private, 27, 544
public, 27,544
public-key vs. symmetric-key, 31-32, 551
recovery, 580
registration, 579
revocation, 566,580
secret, 544
separation, 567
short-term, 553
symmetric, 544
terminal, 552
update, 580
variant, 568
Key access server, 549
Key agreement, 34, 35, 505-506, 515-524, **536–** *538*
Blom's key pre-distribution system, 506
definition of, 490
Diffie-Hellman, 5 16
ElGamal, 5 17
encrypted key exchange (EKE), 538
Gunther, 522
MTI/A0, 5 17-5 19
relation to key transport, 49 1
Station-to-station (STS), 519
Key authentication, 492
Key clustering attack on block ciphers, 281

RFC 1319,655
MD4 hash function, 346
RFC 1320,655
MD5 hash function, 347
RFC 1321,655
MDS-MAC, 358
MDC-2 hash function, 342
ISO/IEC 10118-2 standard, 647
patent, 639
MDC-4 hash function, 343
patent, 639
MDS code, 281,506
Mean, 5 1
Measure of roughness, 249
Mechanism, 34
Meet-in-the-middle attack
on double DES, 235
on double encryption, 235
time-memory tradeoff, 236
on multiple encryption
time-memory tradeoff, 236
Meet-in-the-middle chaining attack, 374
Merkle channel, 48
Merkle one-time signature scheme, 464–466, 485
authentication tree, 466
key generation, 464
patent, 643
security of, 465
signature generation, 465
signature verification, 465
Merkle puzzle scheme, 47, 537
Merkle's DES-based hash function, 338, 339, 378
Merkle's meta-method for hashing, 333
Merkle-Hellman knapsack encryption, 300–302, 317–318
basic
decryption algorithm, 301
encryption algorithm, 301
key generation, 300
multiple-iterated
key generation, 302
patent, 637
security of, 302
Mersenne number, 142
Mersenne prime, 142
Message authentication, see Data origin authentication
Message authentication code (MAC), 33,323,352-359,381-383
applications of, 323,330
based on block ciphers, 353-354
CBC-MAC, see CBC-MAC
CFB-64 MAC, 650
RIPE-MAC, see RIPE-MAC
birthday attack on, 352
customized, 356-358
bucket hashing, 382
MDS-MAC, 358
Message Authenticator Algorithm (MAA), 356
definition, 325
for stream ciphers, 358-359
CRC-based, 359
Lai-Rueppel-Woollven scheme, 383
Taylor's scheme, 383
from MDCs, 354-355
envelope method with padding, 355
hash-based MAC, 355
HMAC, 355
secret prefix method, 355
secret suffix method, 355
XOR MAC, 382
IS0 8730 standard, 652
IS0 9807 standard, 652
properties of
compression, 325
computation-resistance, 325
ease of computation, 325
key non-recovery, 325
retail MAC, 650
types of attack
adaptive chosen-text, 326
chosen-text, 326
known-text, 326
types of forgery
existential, 326
selective, 326
see *also* CBC-MAC
Message authentication tag system, 376
Message Authenticator Algorithm (MAA), 356
IS0 873 l-2 standard, 652
Message concealing in RSA, 290, 3 13
Message digest, 321
Message integrity code (MIC), 323
Message space, 11
Message-independent key establishment, 493
Micali-Schnorr pseudorandom bit generator, 186
Miller-Rabin primality test, 139, 165
MIME, 656,661
Minimum disclosure proof, 421
Minimum polynomial, 156
Mips year, 126
Mixed-radix representation, 611,630
Mixing algebraic systems, 279
Miyaguchi-Preneel hash function, 341
Mobius function, 154
mod notation, 64
Modes of operation

KryptoKnight, 535, 541
KTC, see Key translation center (KTC)

L
L^3-lattice basis reduction algorithm, 118-120, 131
Lagrange's theorem, 76
Lambda method for discrete logarithms, 128
Lamport's one-time-password scheme, 396
Lanczos method, 129
Lattice, 118
  dimension of, 118
  reduced basis, 118
Lattice basis reduction algorithm, 118-120, 131,317
Law of large numbers, 52
Law of quadratic reciprocity, 72
lcm, see Least common multiple
Leading coefficient, 78
LEAF, 584-585
Leaf of a binary tree, 557
Least common multiple, 64
Least significant digit, 593
Legendre symbol, 72
  computing, 73
Lehmer's gcd algorithm, 607–608, 632
Length of a vector, 118
Liar, 135
  Euler, 138
  Fermat, 136
  strong, 139
Life cycle, see Key life cycle
Linear code, 506
Linear combination, 80
Linear complexity, 198-201
  algorithm for computing, see Berlekamp-Massey algorithm
  of a finite sequence, 198
  of a random periodic sequence, 199
  of a random sequence, 198
  of an infinite sequence, 198
  profile, 199
Linear complexity profile, 199-200
  algorithm for computing, 201
  limitations of, 200
  of a random sequence, 199
Linear congruential generator, 170, 187
  multivariate congruential generator, 187
  truncated, 187
Linear consistency attack, 219-220
Linear cryptanalysis
  of block ciphers, 258, 271,278, 280
  of stream ciphers, 219
Linear feedback shift register (LFSR), 195-201
  connection polynomial of, 196
  definition of, 195
  delay element of, 195
  feedback bit of, 196
  initial state of, 196
  maximum-length, 197
  non-singular, 196
  output sequence of, 195
  stage of, 195
Linear sieve, 128
Linear syndrome attack, 218
Linearly dependent, 80
Linearly independent, 80
LION block cipher, 282
Little-endian, 344
Lock-in, 221
LOKI block cipher, 281
  LOKI'89, 281
  LOKI'91, 270, 281
Long-term key, 553
Low-order digit, 593
Luby-Rackoff block cipher, 282
LUC cryptosystem, 314
  LUCDIF, 3 16
  LUCELG, 3 16
Lucas-Lehmer primality test, 142
Lucifer block cipher, 276
  patent, 641,659

M
m-sequence, 197
MAC, see Message authentication code (MAC)
Manipulation detection code (MDC), 323
Mapping, 6
Markov cipher, 280
MASH-l hash function, 352
  ISO/IEC 10118-4 standard, 647
MASH-2 hash function, 352
  ISO/IEC 10118-4 standard, 647
Master key, 55 1
Matyas-Meyer-Oseas hash function, 341
  ISO/IEC 10118-2 standard, 647
Maurer's algorithm for provable prime generation, 153, 167
Maurer's universal statistical test, 183-185, 189
Maximum order complexity, 217
Maximum-length LFSR, 197
Maximum-rank-distance (MRD) code, 317
McEliece public-key encryption, 298-299, 3 17
  decryption algorithm, 299
  encryption algorithm, 299
  key generation, 298
  recommended parameter sizes, 299
  security of, 299
MD-strengthening, 334, 335, 337
MD2 hash function, 380

filtering function, 208
Nonlinear order, 205
Normal basis, 168
exponentiation, 642
multiplication, 642
patents, 642-643, 659
Normal distribution, 176-177
mean of, 176
standard, 176
variance of, 176
Normal polynomial, 168
Normalization, 599
Notarized key, 569
Notary
agent, 550
seal, 569
service, 582
Number field sieve
for discrete logarithms, 128
for integer factorization, 98, 126
implementation reports, 126, 127
general number field sieve, 98
special number field sieve, 98, 126
Number theory, 63-75
Nyberg-Rueppel signature scheme, 460462,485
security of, 461
signature generation, 461
signature verification, 461

0

Object identifier (OID), 660
OFB, see Output feedback mode
Off-line trusted third party, 548
Ohta-Okamoto identification protocol, 422
On-line certificate, 576
On-line trusted third party, 547
On-line/off-line signature, 486
patent, 644
One-key encryption, 15
One-sided statistical test, 179
One-time insider, 496
One-time pad, 21, 192-193, 274
patent, 657
One-time password scheme, 395-397
One-time signature scheme, **462–471**
Diffie-Lamport, 485
GMR, **468–47** 1
Merkle, 464-466
Rabin, 462-464
validation parameters, 462
One-to-one function, 7-8
One-way cipher, 377
One-way function, **8–9, 327**
DES-based, 190,328
exponentiation modulo a prime, 115, 329
multiplication of large primes, 329
Rabin function, 115
RSA function, 115
One-way hash function (OWHF), 325
One-way permutation, 328
Onto function, 7
Open Systems Interconnection (OSI), 653, 660
Operational, 532
Opponent, 13,495
see *also* Attacker
Optimal normal basis, 168,659
Order
generating element of maximum order in $\mathbb{Z}_n^*$, 163
of $\mathbb{Z}_n^*$, 69
of a finite field, 80
of a group, 75
of a group element, 76, 160
algorithm for determining, 162
of an element in $\mathbb{Z}_n^*$, 69
Otway-Rees protocol, 504,536
Output feedback mode (OFB), 232-233
as a stream cipher, 233
changing IV in, 232
counter mode, 233
feedback size, 233
Outsider, 496
Ownership, 3

P

Palindromic keys of DES, 257
Party, 13
Passcode generator, 402
Passive adversary, 15
Passive attack, 41,495
Passkey, 395
Passphrase, 390
Passwords (weak authentication), **388–397, 420**
aging, 390
attacks on, 391-393
dictionary, 392
exhaustive search, 391
password-guessing, 392
pre-play, 397
replay, 391
encrypted password file, 389
entropy, 392
generator, 387
one-time, 395-397
Lamport's scheme, 396
passkey, 395
passphrase, 390
personal identification number (PIN), 394

multiple modes, see Multiple encryption, modes of operation
single modes, see Block cipher, modes of operation
Modification detection code, 33, 323
Modified-Rabin pseudorandom bit generator, 190
Modified-Rabin signature scheme, 439442,482
key generation, 440
security of, 441
signature generation, 440
signature verification, 440
Modular arithmetic, see Multiple-precision modular arithmetic
Modular exponentiation, see Exponentiation
Modular reduction, 599
Barrett, **603–605, 63** 1
Montgomery, **600–602, 631**
special moduli, 605-606
Modular representation, see Mixed-radix representation
Modulus, 67
Monic polynomial, 78
Mono-alphabetic substitution cipher, see Substitution cipher
Monotone access structure, 527
Montgomery exponentiation, 619-620
Montgomery multiplication, 602-603
Montgomery reduction, **600–602**, 631
MOSS, 656
RFC 1848,656
Most significant digit, 593
MTI protocols, 518,537
MTI/A0 key agreement, **517–519, 537**
Goss variant, 537
patent, 644, 659
Multi-secret threshold scheme, 527
Multiple encryption, 234-237
definition of, 234
double encryption, 234
modes of operation, 237
triple-inner-CBC mode, 237
triple-outer-CBC mode, 237
triple encryption, 235
E-D-E, 235
two-key triple-encryption, 235
Multiple polynomial quadratic sieve, 97
Multiple-precision integer, 593
Multiple-precision integer arithmetic, 592-599
addition, 594-595
division, 598-599
normalization, 599
gcd, see Greatest common divisor
multiplication, 595-596
discrete Fourier transform **(DFT)**, 63 1
Karatsuba-Ofman, 630
squaring, 596-597
subtraction, 594-595
Multiple-precision modular arithmetic, **599–606**
addition, 600
exponentiation, see Exponentiation
inversion, 610
multiplication
classical, 600
Montgomery multiplication, 602-603
reduction, 599
Barrett, **603–605, 631**
Montgomery, **600–602, 63** 1
special moduli, 605-606
subtraction, 600
Multiplexer generator, 220
Multiplicative group
of $\mathbb{Z}_n$, 69
of a finite field, 8 1
Multiplicative inverse, 68
computing, 71, 84,610
Multiplicative property in RSA, **288, 435, 482**
Multiplicity of a factor, 122
Multispeed inner-product generator, 220
Multivariate polynomial congruential generator, 187
Mutual authentication, **387, 402, 405, 494**
Mutual information, 57
Mutually exclusive events, 51

N

N-Hash function, 380
Name server, 549
Needham-Schroeder public-key, 508,536
Needham-Schroeder shared-key, **401, 503, 535**
Next-bit test, 171
Next-discrepancy, 200
Nibble, 443
NIST, 654
Noise diode, 40
Non-interactive protocol, 493
Non-interactive ZK proof, 424
Non-malleable encryption, 3 11, 3 19
Non-repudiation, **3, 4,** 582-584
ISO/IEC 13888 standard, 648
Non-singular
FSR, 203
LFSR, 196
Nonce, 397,497
Nonlinear combination generator, 205-208
combining function of, 205
Nonlinear feedback shift register, see Feedback shift register (FSR)
Nonlinear filter generator, 208-209

incremental search, 148
provable primes, 152-154
random search, 145-149
strong primes, 149-150
Prime number theorem, 64
Primitive element, see Generator
Primitive normal polynomial, 168
Primitive polynomial, 157-160
algorithm for generating, 160
algorithm for testing, 157
definition of, 84
Primitives, 4
Principal, 495
Principal square root, 74
Privacy, see Confidentiality
Privacy Enhanced Mail (PEM), 588,655
RFCs 1421–1424, 655
Private key, **26, 27, 544**
Private-key certificate, see Symmetric-key certificate
Private-key encryption, 15
Probabilistic public-key encryption, **306–312, 318–319**
Blum-Goldwasser, 308-3 11
Goldwasser-Micali, 307-308
security level
polynomially secure, 306
semantically secure, 306
Probability, 50
Probability density function, 176
Probability distribution, 50
Probability theory, **50–55**
Probable prime, 136
Product cipher, 20,251
Proof of knowledge, **406, 421, 422**
Proposed Encryption Standard (PES), 279
Protection lifetime, 553,578
Protocol
authentication, 493
cut-and-choose, 410,421
definition of, 33,490
failure of, 34
hybrid, 5 12
identification, see Identification
key establishment, see Key establishment
message-independent, 493
non-interactive, 493
witness hiding, 423
zero-knowledge, 405-417
Provable prime, 134, 142
Provable security, 43,533
Prover, 386
Pseudo-collision, 371
Pseudo-Hadamard transform, 266
Pseudo-noise sequence, 18 1
Pseudoprime, 136
Euler, 138
strong, 139
Pseudorandom bit generator (PRBG), 173-175
ANSI X9.17, 173
definition of, 170
FIPS 186, 174–175
linear congruential generator, 170, 187
Pseudorandom bit sequence, 170
Pseudorandom function, 33 1
Pseudorandom sequences, **39–41**
Pseudosquares modulo n, **74, 99**
Public key, **26, 27, 544**
compared vs. symmetric-key, 31-32,551
implicitly-certified, 520-522
Public-key certificate, **39, 559–561,** 587
data part, 559
distinguished name, 559
signature part, 559
Public-key encryption, 25-27, 283-319
advantages of, 3 1
disadvantages of, 32
ElGamal, 294-298
knapsack, 300-306
Chor-Rivest, 302-306
Merkle-Hellman, 300-302
LUC, see LUC cryptosystem
McEliece, 298-299
non-malleable, 3 11
plaintext-aware, 3 1 l-3 12
probabilistic, 306-312
Blum-Goldwasser, 308-3 11
Goldwasser-Micali, 307-308
Rabin, 292-294
reversible, 28
RSA, 285-291
types of attacks, 285
Williams, 315
PURPLE cipher, 276
Puzzle system, 376,537

Q

Quadratic congruential generator, 187
Quadratic non-residues, 70
Quadratic residues, 70
Quadratic residuosity problem, 99, 127, 307
Quadratic sieve factoring algorithm, 95-97, 126
implementation reports, 126
Quantum computer, 130
Quantum cryptography, 48,535
Quotient, **64, 78**

R

Rabin one-time signature scheme, **462–464**

rules, 389
salting, 390
stored password file, 389
UNIX, 393-394
Patents, 635-645, 657-659
ordering and acquiring, 645
priority date, 636
validity period, 636
PEM, see Privacy Enhanced Mail (PEM)
Pepin's primality test, 166
Perceptrons problem, 423
Perfect forward secrecy, 496,534
Perfect power
testing for, 89
Perfect secrecy, 42,227
Perfect secret sharing scheme, 526, 527
Perfect zero-knowledge protocol, 407
Period of a periodic sequence, 180
Periodic sequence, 180
autocorrelation function of, 180
cycle of, 180
period of, 180
Permanent insider, 496
Permutation, 10
Permutation polynomial, 3 14
Permuted kernel problem, 423
Personal Identification Number (PIN)
ANSI X9.8 standard, 649
IS0 9564 standard, 652
PGP, see Pretty Good Privacy (PGP)
Phi function (ϕ), 65
Photuris, 661
Physically secure channel, 13
PIKE stream cipher, 222
PIN, see Passwords (weak authentication), see Personal Identification Number (PIN)
PKCS standards, 656,661
ordering and acquiring, 657
PKCS #1, 44547,483
Plaintext, 11
Plaintext-aware encryption scheme, 3 11-312
Playfair cipher, 239, 274
Pless generator, 218
PN-sequence, 18 1
Pocklington's theorem, 144
Pohlig-Hellman algorithm, 107-109, 128
Pohlig-Hellman cipher, 27 1
patent, 642, 659
Poker test, 182, 188
Policy Certification Authority (PCA), 589
Pollard's $p-1$ algorithm, 92-93, 125
Pollard's rho algorithm
for discrete logarithms, 106–107, 128
for factoring, 91-92, 125
Polyalphabetic substitution cipher, 18, 241-242, 273-274
auto-key cipher, 242
Beaufort cipher, 241
cipher machine, see Cipher machine
PURPLE cipher, 276
Vigenere cipher
auto-key, 242
compound, 241
full, 242
running-key, 242
simple, 18,241
single mixed alphabet, 242
Polygram substitution cipher, 239
Polynomial, 78
irreducible, 78
leading coefficient of, 78
Polynomial basis, 83
Polynomial factorization, 122-124, 132
Berlekamp's Q-matrix algorithm, 124
square-free factorization, 123
Polynomial-time algorithm, 59
Polynomial-time statistical test, 171
Polynomially security public-key encryption, 306
Polytime reduction, 61, 88
Practical security, 43
Pre-play attack, 397,398
Pre-positioned secret sharing scheme, 527
Precision, 593
Preimage, 6
Preimage resistance, 323
Pretty Good Privacy (PGP), 661
Primality proving algorithm, see Primality test, true primality test
Primality test
probabilistic primality test, 135-142
comparison, 140-142
Fermat's test, 136
Miller-Rabin test, 139
Solovay-Strassen test, 138
true primality test, 142-145
Atkin's test, 145
Goldwasser-Kilian test, 166
Jacobi sum test, 144
Lucas-Lehmer test, 142
Pepin's test, 166
Prime number, 9, 64
Prime number generation, 145-154
algorithms
Gordon's algorithm, 150
Maurer's algorithm, 153
NIST method, 151
random search, 146
DSA primes, 150-152

- RSA problem, 98-99, 127,287
  - security of individual bits, 116
- RSA pseudorandom bit generator, 185-186
- RSA public-key encryption, 285-29 1, 3 12-3 15
  - decryption algorithm, 286,611, 613
  - decryption exponent, 286
  - elliptic curve analogue, 3 15
  - encryption algorithm, 286
  - encryption exponent, 286
  - key generation, 286
  - modulus, 286
  - patent, 638
  - prime selection, 290
  - recommended modulus size, 290
  - security of, 287-290
    - adaptive chosen-ciphertext attack, **289, 3** 13
    - common modulus attack, 289
    - cycling attacks, 289, 3 13
    - forward search attack, 288
    - message concealing, **290, 3** 13
    - multiplicative properties, 288
    - polynomially related plaintext, 3 13
    - relation to factoring, 287
    - small decryption exponent, 288
    - small encryption exponent, 288, 291, 3 13
  - unbalanced, 314
- RSA signature scheme, **433–438, 482**
  - ANSI X9.31-1 standard, 651
  - bandwidth efficiency, 437
  - **ISO/IEC 9796, 442–444**
  - key generation, 434
  - patent, 638
  - PKCS **#1, 445–447**
  - reblocking problem, 435436,482
  - redundancy function, 437
  - security of, 434-435
  - signature generation, 434,613
  - signature verification, 434
- Run of a sequence, 180
- Running key generator, 194
- Runs test, 182, 188

S

- S/MIME, 66 1
- Safe prime, 537
  - algorithm for generating, 164
  - definition of, 164
- SAFER block cipher, 266-269, 280
  - attacks on, 280
  - SAFER K-64 decryption algorithm, 269
  - SAFER K-64 encryption algorithm, 268
  - SAFER K-64 key schedule, 268
  - SAFER K-128,280
  - SAFER SK-64 key schedule, 268
  - SK-128,280
  - test vectors, 269
- Salt, 390
- Schnorr identification protocol, **414–416, 422**
  - patent, 639
- Schnorr signature scheme, **459–460, 484**
  - **Brickell-McCurley** variant, 484
  - Okamoto variant, 484
  - patent, 639
  - signature generation, 459
  - signature verification, 460
- SEAL stream cipher, 213-216
  - implementation report, 222
  - patent, 222
  - test vectors, 2 15
- Sealed authenticator, 361
- Sealed key, 568
- **2nd-preimage** resistance, 323,325
- Secrecy, see Confidentiality
- Secret broadcasting scheme, 540
- Secret key, 544
- Secret-key certificate, 588
- Secret sharing, **524–528, 538–540**
  - access structure, 526
  - authorized subset, 527
  - dynamic, 527
  - extendable, 526
  - generalized, 526-528
  - ideal, 527
  - information rate, 527
  - multi-secret threshold, 527
  - perfect, 526, 527
  - pre-positioned, 527
  - ramp schemes, 539
  - shared control schemes, 524-525
  - threshold scheme, 525-526
  - verifiable, 527
  - visual cryptography, 539
  - with disenrollment, 528
- Secure channel, 13
- Secure Hash Algorithm **(SHA-1),** 348
  - ANSI X9.30-2 standard, 65 1
  - FIPS **180-** 1 standard, 654
  - **ISO/IEC** 10118-3 standard, 647
- Secured channel, 13
- Security domain, 570
- Security policy, 545
- Seed, 21, 170
- Selective forgery, 432
- Self-shrinking generator, 221
- Self-synchronizing stream cipher, 194-195
- Semantically secure public-key encryption, 306
- Semi-weak keys of DES, 257
- Sender, 13

Sequence
- block of, 180
- de **Bruijn**, 203
- gap of, 180
- m-sequence, 197
- periodic, 180
- pn-sequence, 18 1
- pseudo-noise, 18 1
- run of, 180

Sequence numbers, 399
Serial test, 181, 188
Session key, 36,494
Session key establishment, 491
SHA-1, see Secure Hash Algorithm (SHA-1)
Shamir's no-key protocol, 500,535
Shamir's threshold scheme, 526, 539
Shared control schemes, 524-525
SHARK block cipher, 281
Shift cipher, 239
Short-term key, 553
Shrinking generator, 211-212
- implementation report, 221

Sieving, 97
Signature, **3, 22–23, 28–30, 425–488**
- arbitrated, **472–473**
- blind, see Blind signature scheme
- designated confirmer, 487
- deterministic, 427
- Diffie-Lamport, 485
- Digital Signature Algorithm (DSA), **452–454**
- ElGamal, **454–459**
- ESIGN, 473-474
- fail-stop, see Fail-stop signature scheme
- Feige-Fiat-Shamir, 447-449
- framework, **426–433**
- generation algorithm, 426
- GMR, 468-47 1
- GQ, **450–45** 1
- group, 488
- handwritten, 23
- Merkle one-time, 464466
- modified-Rabin, **439–442**
- Nyberg-Rueppel, 460-462
- on-line/off-line, 486
- Ong-Schnorr-Shamir (OSS), 482,486
- Rabin, 438-442
- Rabin one-time, **462–464**
- randomized, 427
- relation to identification, 388
- resolution of disputes, 30
- RSA, **433–438**
- Schnorr, **459–460**
- strongly equivalent, 485
- types of attacks, 432
- undeniable, see Undeniable signature scheme
- verification algorithm, 426
- with appendix, 481
  - framework, **428–430**
  - **ISO/IEC** 14888 standard, 648
  - PKCS **#1, 445–447**
- with message recovery, 29
  - framework, 430-432
  - **ISO/IEC** 9796 standard, 4424,646, 660
- with redundancy, 29

Signature notarization, 583
Signature space, 427
Signature stripping, 510
Signed-digit representation, 627-628
Signed-magnitude representation, 593
Signer, 23
Significance level, 179
Signing transformation, 22
Simple substitution cipher, see Mono-alphabetic substitution cipher
Simulator, 407
Simultaneous diophantine approximation, 121-122
- algorithm for, 122
- unusually good, 12 1

Simultaneous multiple exponentiation, 617
Simultaneously secure bits, 115
Single-key encryption, 15
Single-length MDC, 339
Single-precision integer, 593
Singleton bound, 506
SKEME, 661
SKID2 identification protocol, 402,421
SKID3 identification protocol, 402,421
SKIP, 661
SKIPJACK block cipher, 282,654
Sliding-window exponentiation, 616
Small decryption exponent in RSA, 288
Small encryption exponent in RSA, **288, 291, 3** 13
Smart card, 387
- IS0 10202 standard, 652

Smooth
- integer, 92
- polynomial, 112

Snefru hash function, 380
- 8 x 32 S-boxes, 281

Solovay-Strassen primality test, 138, 165
Sparse linear equations, 129
- conjugate gradient method, 129
- Lanczos method, 129
- Wiedemann algorithm, 129

Special-purpose factoring algorithm, 90
SPKM, 656,661

- Split-knowledge scheme, 525
- Splitting an integer, 89
- Spread spectrum, 45
- Square roots, 99-102
  - composite modulus, **101–102,** 127
  - prime modulus, 100-101, 127
  - SQROOT problem, 101
- Square-free factorization, 123
  - algorithm for, 123, 132
- Square-free integer, 137
- Square-free polynomial, 123
- Stage
  - of an FSR, 202
  - of an LFSR, 195
- Standard deviation, 51
- Standard normal distribution, 176
- Standards, **645–657, 660–661**
  - ANSI, 648-65 1
  - FIPS, 654-655
  - IEEE, 660
  - Internet, 655-656
  - **ISO/IEC, 645–648, 651–653**
  - PKCS, 656
  - RFC, 655-656
  - X.509,653
- Station-to-station (STS) key agreement, 519,538
- Statistical test, 175-185, 188-189
  - autocorrelation test, 182
  - frequency test, 181
  - hypothesis, 179
  - Maurer's universal statistical test, 183-185, 189
  - one-sided test, 179
  - poker test, 182
  - polynomial-time, 171
  - runs test, 182
  - serial test, 181
  - significance level, 179
  - two-sided test, 180
- Statistical zero-knowledge protocol, 424
- Steganography, 46
- Step-l/step-2 generator, 220
- Stirling numbers, 53
- Stirling's formula, 59
- Stop-and-go generator, 220
- Stream cipher, 20-21, 191-222
  - attacks on
    - correlation attack, 206, 218
    - inversion attack, 219
    - linear consistency attack, 219-220
    - linear cryptanalysis, 219
    - linear syndrome attack, 218
    - lock-in, 221
  - cellular automata, 222
  - classification, 192-195
  - clock-controlled generator, 209-212
    - alternating step generator, 209-211
    - m-sequence cascade, 221
    - p-cycle cascade, 220
    - self-shrinking generator, 221
    - shrinking generator, 211-212
    - step-l/step-2 generator, 220
    - stop-and-go generator, 220
  - comparison with block ciphers, 192
  - FISH, 222
  - GOAL, 219
  - initial state, 193, 194
  - keystream, 193, 194
  - next-state function, 193
  - nonlinear combination generator, 205-208
    - Geffe generator, 206
    - multiplexer generator, 220
    - multispeed inner-product generator, 220
    - **Pless** generator, 2 18
    - summation generator, 207
  - nonlinear filter generator, 208-209
    - knapsack generator, 209
  - one-time pad, 192-193
  - output function, 193, 194
  - PIKE, 222
  - randomized stream cipher, 216
  - **RC4, 222**
  - Rip van Winkle cipher, 216
  - SEAL, 213-216
  - self-synchronizing stream cipher, 194-195
  - synchronous stream cipher, 193-194
- Strict avalanche criterion (SAC), 277
- String-replacement representation, 628-629
- Strong collision resistance, 324
- Strong equivalent signature schemes, 485
- Strong liar, 139
- Strong one-way hash function, 325
- Strong prime, 149-150
  - algorithm for generating, 150
  - definition of, 149,291
  - Hellman-Bach patent, 643
  - usage in RSA, 291
- Strong pseudoprime, 139
- Strong pseudoprime test, see Miller-Rabin primality test
- Strong witness, 139
- Subexponential-time algorithm, 60
- Subfield, 77
- Subgroup, 76
- Subliminal channel, 485
  - broadband, 485
  - narrowband, 485
- Subset sum problem, 61, 117-122, 190
  - meet-in-the-middle algorithm, 118

    naive algorithm, 117
    superincreasing, 300
    using L^3 algorithm, 120
Subspace of a vector space, 80
Substitution cipher, 17-18, 238-241
    homophonic, 17,240
    mono-alphabetic, 17,239
        affine cipher, 239
        Caesar cipher, 239
        shift cipher, 239
        unicity distance of, 247
    polyalphabetic, 18
    polygram, 239
        Hill cipher, 240
        Playfair cipher, 239
Substitution-permutation (SP) network, 251
Summation generator, 207, 218
Superincreasing subset sum problem, 300
    algorithm for solving, 300
Superuser, 389
Surjective function, 46
SWIFT, 586
Symmetric cryptographic system, 544
Symmetric key, 544
    compared vs. public-key, 3 l-32, 55 1
Symmetric-key certificate, 554–555, 587
Symmetric-key encryption, 15-21
    advantages of, 3 1
    block cipher, 223-282
    definition of, 15
    disadvantages of, 3 1
    stream cipher, 191-222
Synchronous stream cipher, 193-194
    binary additive stream cipher, 194
Syndrome decoding problem, 190,423

T

Tapper, 13
TEA block cipher, 282
TEMPEST, 45
Teraflop, 44
Terminal key, 552
Test vectors
    DES, 256
    FEAL, 262
    IDEA, 265
    MD4, 345
    MD5, 345
    MD5-MAC, 358
    RC5, 270
    RIPEMD-160,345
    SAFER, 269
    SHA-1,345
3-WAY block cipher, 281
Threshold cryptography, 534
Threshold scheme, 525-526
    Blakley, 538
    Shamir, 526,539
Ticket, 501, 570, 586
Time-variant parameter, 362, 397–400, 497
    nonce, 397
    random numbers, 398-399
    sequence numbers, 399
    timestamps, 399-400
Timestamp, 3, 399–400, 420, 581–582
    agent, 550
Toeplitz matrix, 382
Transaction authentication, 362
Transformation, 6
Transinformation, 57
Transposition cipher, 18, 238
    compound, 238
    simple, 18,238
    unicity distance of, 246
Trapdoor one-way function, 9, 26
Trapdoor predicate, 3 18
Tree authentication, 376
    patent, 637
Trinomial, 154
Triple encryption, 235-237, 272
Triple-DES, 272, 65 1
    ANSI X9.52 standard, 651
Triple-inner-CBC mode, 237
Triple-outer-CBC mode, 237
Truncated differential analysis, 271, 280
Trust model, 572
    centralized, 573
    directed graph, 575
    distributed, 575
    hierarchy with reverse certificates, 575
    rooted chain, 573
    separate domains, 573
    strict hierarchical, 573
Trusted server, 491
Trusted third party (TIP), 30, 36, 491, 547-550, 581-584
    authentication server, 549
    certificate directory, 549
    certification authority (CA), 548
    functionally trusted, 39
    in-line, 547
    KDC, see Key distribution center (KDC)
    key access server, 549
    key escrow agent, 550
    key generator, 549
    key management facility, 549
    key server, 549
    KTC, see Key translation center (KTC)

name server, 549
notary agent, 550
off-line, 548
on-line, 547
registration authority, 549
timestamp agent, 550
unconditionally trusted, 39
TTP, see Trusted third party (TTP)
Turing-Kolmogorov-Chaitin complexity, 217
Two's complement representation, 594
2-adic span, 218
Two-key triple-encryption, 235
chosen-plaintext attack on, 236
known-plaintext attack on, 237
Two-sided statistical test, 180
Type I error, 179
Type II error, 179

U

Unbalanced RSA, 314
Unblinding function, 475
Unconcealed message, 290
Unconditional security, see Perfect secrecy, 533
Unconditionally trusted third party, 39
Undeniable signature scheme, **476–478**, **487–488**
Chaum-van Antwerpen, 476-478
confirmer, 487
Unicity distance
definition of, 246
known-plaintext, 235
of a cascade cipher, 272
of a mono-alphabetic substitution cipher, 247
of a transposition cipher, 246
Unilateral authentication, **387**, **401–402**, **405**, **494**
Union of sets, 49
Unique factorization domain, 81
Universal classes of hash function, 376
Universal exponent, 287
Universal forgery, 482
Universal one-way hash function, 377
Universal statistical test, see Maurer's universal statistical test
UNIX passwords, 393-394
Unsecured channel, 13
Unusually good simultaneous diophantine approximation, 121,317
Userid, 388

V

Validation, 3
Validation parameters, 462
Variance, 5 1
Vector space, 79-80
dimension of, 80
standard basis, 80
subspace of, 80
Vector-addition chains, 622-623
Verifiable secret sharing, 527, 539
Verification algorithm, 426
Verification transformation, 22
Verifier, **23**, **385**, **386**
Vernam cipher, see One-time pad
Vigenere cipher, see Polyalphabetic substitution cipher
Visual cryptography, 539

W

WAKE block cipher, 282
Weak collision resistance, 324
Weak keys of DES, 257
Weak one-way hash function, 325
Wheatstone disc, 274
Wholesale banking, 648
Wiedemann algorithm, 129
Williams' public-key encryption, 3 15
Witness, 135,409
Euler, 137
Fermat, 136
strong, 139
Witness hiding protocol, 423
Witness indistinguishability, 423
Witnessing, 3
Work factor, **44**
historical, 44
Worst-case running time, 58
Wyner's wire-tap channel, 535

X

X.509 authentication protocol, 536
three-way, 5 12
two-way, 511
X.509 certificate, 587
X.509 standard, 653

Y

Yuval's birthday attack, 369

Z

Zero-knowledge identification, **405–417**, **421–424**
Brickell-McCurley, 423
comparison of protocols, **416–417**
constrained linear equations problem, 423
extended Fiat-Shamir, 422
Feige-Fiat-Shamir, **410–412**
Fiat-Shamir (basic version), 408
Fischer-Micali-Rackoff, 422
GQ, **412–414**
Ohta-Okamoto, 422
permuted kernel problem, 423
Schnorr, 414-416

- syndrome decoding problem, 423

Zero-knowledge protocol, **405–417, 421–424**
- auxiliary-input, 423
- black-box simulation, 423
- challenge, 409
- completeness, 406
- computational, 407
- extracting secret, 406
- for possession of discrete log, 422
- parallel version, 412
- perfect, 407
- proof of knowledge, **406, 421, 422**
- proof of membership, 421
- response, 409
- simulator, 407
- soundness, 406
- statistical, 424
- witness, 409

Ziv-Lempel complexity, 217

&,-operation, 82