Appendix A

Bibliography of Papers from Selected Cryptographic Forums

Contents in Brief

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,* 451–462.
M.H.G. Anthony, K.M. Martin, J. Seberry, P. Wild, *Some remarks on authentication systems,* 122–139.
L. Brown, J. Pieprzyk, J. Seberry, *LOKI – 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,* 426–432.
C. Ding, *Lower bounds on the weight complexities of cascaded binary sequences,* 39–43.
R. Ferreira, *The practical application of state of the art security in real environments,* 334–355.
K. Gaarder, E. Snekkenes, *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 flexible untraceable electronic cash,* 294–305.

©1997 CRC Press LLC

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. Müller, *A note on strong Fibonacci pseudoprimes,* 311–317.

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 of pseudo-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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

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. Harn, H.-Y. Lin, *An oblivious transfer protocol and its application for the exchange of secrets,* 312–320.

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. Stern, *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.

©1997 CRC Press LLC

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

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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,* 479–491.

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 among preimages 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,* 231–243.

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

J. Sauerbrey, *A modular exponentiation unit based on systolic arrays,* 505–516.

J. Seberry, X.-M. Zhang, *Highly nonlinear 0-1 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. Seberry, *HAVAL – a one-way hashing algorithm with variable length of output,* 83–104.

E. Zuk, *Remarks on "The design of a conference key distribution system",* 467–468.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

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, P.C. Leyland, *The magic words are SQUEAMISH OSSIFRAGE,* 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.

©1997 CRC Press LLC

E. Biham, A. Biryukov, *How to strengthen DES using existing hardware,* 398–412.
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),* 427–430.
X. Chang, Z.-D. Dai, G. Gong, *Some cryptographic properties of exponential functions,* 415–418.
C. Charnes, 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 nonperfect 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. Stern, *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^2DES,* 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. Karnin, J.M. Reyneri, *Compact knapsacks are polynomially solvable* (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 flipping by telephone: A protocol for solving impossible problems,* 11–15.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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* $\mathrm{GF}(2^p)$*,* 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 of ping-pong protocols,* 177–186.

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

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

S. Even, O. 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,* 129–131.

M.E. Hellman, J.M. Reyneri, *Fast computation of discrete logarithms in* $\mathrm{GF}(q)$*,* 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 of public-key cryptography for signing checks,* 187–197.

M. Merritt, *Key reconstruction,* 321–322.

C. Mueller-Schloer, N.R. Wagner, *Cryptographic protection of personal data cards,* 219–229.

C. Nicolai, *Nondeterministic cryptography,* 323–326.

J.B. Plumstead, *Inferring a sequence produced by a linear congruence,* 317–319.

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. Winternitz, *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, O. Goldreich, *Electronic wallet,* 383–386.

S. Even, O. Goldreich, *On the power of cascade ciphers,* 43–50.

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

O. Goldreich, *A simple protocol for signing contracts,* 133–136.

H. Jürgensen, 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. Müller, *Permutation polynomials in RSA-cryptosystems,* 293–301.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

H. Ong, C.P. Schnorr, *Signatures through approximate respresentations by quadratic forms,* 117–131.
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 and performance 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. Winternitz, *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,* 475–480.
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,* 481–485.
D. Chaum, *New secret codes can prevent a computerized big brother,* 432–433.
S.-S. Chen, *On rotation group and encryption of analog signals,* 95–100.
B. Chor, O. 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. Hoornaert, 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.
O. 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. Hoornaert, 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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

J.A. Reeds, J.L. Manferdelli, *DES has no per round linear factors,* 377–389.
S.C. 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,* 411–431.
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 scheme proposed 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, O. 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,* 516–522.
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, O. Goldreich, A. Shamir, *On the security of ping-pong protocols when implemented using the RSA,* 58–72.
J. Feigenbaum, *Encrypting problem 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),* 212–226.
M. Kochanski, *Developing an RSA chip,* 350–357.
M. Luby, C. Rackoff, *How to construct pseudo-random permutations from pseudo-random functions,* 447.
V.S. Miller, *Use of elliptic curves in cryptography,* 417–426.
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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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,* 409–416.

J. van Tilburg, D.E. Boekee, *Divergence bounds on key equivocation and error probability in cryptanalysis,* 489–513.

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,* 429–432.

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,* 311–323.

P. Beauchemin, G. Brassard, C. Crépeau, 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. Crépeau, 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,* 405–417.

D. Chaum, *Demonstrating that a public predicate can be satisfied without revealing any information about how,* 195–199.

D. Chaum, J.-H. Evertse, *A secure and privacy-protecting protocol for transmitting personal information between organizations,* 118–167.

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

C. Crépeau, *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.

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

O. Goldreich, *Two remarks concerning the Goldwasser-Micali-Rivest signature scheme,* 104–110.

O. 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. Niederreiter, *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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

S. Micali, C. Rackoff, B. Sloan, *The notion of security for probabilistic 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. Rankine, *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,* 393–404.

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,* 461.
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,* 87–119.
C. Crépeau, *Equivalence between two flavours 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-Shamir passport protocol,* 21–39.
F.A. 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.
O. 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,* 40–51.
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 of password security,* 392–397.
Y. Matias, A. Shamir, *A video scrambling technique based on space filling curves,* 398–417.
T. Matsumoto, H. Imai, *On the key predistribution 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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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 of your public key,* 128–134.
Y. Yacobi, *Attack on the Koyama-Ohta identity based key distribution scheme,* 429–433.
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, O. 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. Damgård, *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 fight 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,* 100–117.
O. Goldreich, H. Krawczyk, M. Luby, *On the existence of pseudorandom generators,* 146–162.
O. 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 1-way functions,* 578–579.
R.T.C. Kwok, M. Beale, *Aperiodic linear complexities of de Bruijn sequences,* 479–482.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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 number generators,* 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-forwared 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,* 119–131.

K. Zeng, M. Huang, *On the linear syndrome method in cryptanalysis,* 469–478.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

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, *New paradigms 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, *Addition 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 of periodic 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, O. 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. Karn, *UNIX password security – ten years later,* 44–63.

A. Fiat, *Batch RSA,* 175–185.

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

©1997 CRC Press LLC

O. Goldreich, H. Krawczyk, *Sparse pseudorandom 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. Harn, 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,* 100–112.
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,* 128–136.
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,* 154–163.
W.L. Price, *Progress in data security standardisation,* 620–623.
J.-J. Quisquater, J.-P. Delescaille, *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. Matsuzaki, 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,* 461–480.

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 grandmaster problem,* 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.

©1997 CRC Press LLC

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

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

©1997 CRC Press LLC

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. Stern, *The cryptanalysis of a new public-key cryptosystem based on modular knapsacks,* 204–212.
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,* 457–469.
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 of hyperelliptic cryptosystems,* 267–278.
J. Patarin, *New results on pseudorandom permutation generators based on the DES scheme,* 301–312.
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,* 242–251.
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 of participants 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,* 305–311.
A. Beimel, B. Chor, *Universally ideal secret sharing schemes,* 183–195.
M. Bellare, O. 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,* 487–496.
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 of secret sharing schemes,* 148–167.
C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, *Perfectly-secure key distribution for dynamic conferences,* 471–486.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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,* 1–28.
No Author, *Mechanical cryptographic devices,* 47–48.
F.L. 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,* 309–315.
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.
F.C. Piper, *Stream ciphers,* 181–188.
J. Sattler, C.P. Schnorr, *Ein effizienzvergleich der faktorisierungsverfahren von Morrison-Brillhart und Schroeppel,* 331–351.
I. Schaumüller-Bichl, *Cryptanalysis of the Data Encryption Standard by the method of formal 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 transfer protocol,* 379–386.
T. Beth, F.C. 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.
O. Brugia, S. Improta, W. Wolfowicz, *An encryption and authentification procedure for tele-surveillance systems,* 437–445.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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.

O. Goldreich, *On concurrent identification protocols,* 387–396.

O. 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,* 317–334.

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* $0.5 + \epsilon$ *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, *Modeling of encryption techniques for secrecy and privacy in multi-user networks,* 221–230.

J. Bernasconi, C.G. Günther, *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,* 231–240.

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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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,* 167–188.

T. Siegenthaler, *Cryptanalysts representation of nonlinearly filtered ML-sequences,* 103–110.

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 given 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.*

O. 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 formal verification techniques.*

D.S.P. Khoo, G.J. Bird, J. Seberry, *Encryption exponent 3 and the security of RSA.*

J.H. Moore, *Cycle structure of the weak and semi-weak DES keys.*

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

W.B. Müller, 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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

Advances in Cryptology – **EUROCRYPT '88**, Davos, Switzerland. Springer-Verlag LNCS 330 (1988).
Editor: C. Günther.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

Advances in Cryptology – **EUROCRYPT '89**, Houthalen, Belgium. Springer-Verlag LNCS 434 (1990).
Editors: J.-J. Quisquater and J. Vandewalle.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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, O. 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,* 423–428.

C.P. Schnorr, *Efficient identification and signatures for smart cards,* 688–689.

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. Stern, *An alternative to the Fiat-Shamir protocol,* 173–180.

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,* 302–319.

M. Waidner, B. Pfitzmann, *The dining cryptographers in the disco: Unconditional sender and recipient untraceability 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 optimality results on constructing pseudorandom permutations,* 412–422.

Advances in Cryptology – **EUROCRYPT '90**, Aarhus, Denmark. Springer-Verlag LNCS 473 (1991). Editor: I.B. Damgård.

F. Bauspieß, H.-J. Knobloch, P. Wichmann, *Inverting the pseudo exponentiation,* 344–351.

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,* 441–445.

E.F. Brickell, K.S. McCurley, *An interactive identification scheme based on discrete logarithms and factoring,* 63–71.

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,* 1–10.

A.H. Chan, M. Goresky, A. Klapper, *Correlation functions of geometric sequences,* 214–221.

D. Chaum, *Zero-knowledge undeniable signatures,* 458–464.

Z.-D. Dai, T. Beth, D. Gollmann, *Lower bounds for the linear complexity of sequences over residue rings,* 189–195.

©1997 CRC Press LLC

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

Advances in Cryptology – **EUROCRYPT '91**, Brighton, UK. Springer-Verlag LNCS 547 (1991).
Editor: D.W. Davies.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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,* 547–551.

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,* 281–293.

H. Shizuya, T. Itoh, K. Sakurai, *On the complexity of hyperelliptic discrete logarithm problem,* 337–351.

G. Zémor, *Hash functions and graphs with large girths,* 508–511.

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* $\bmod 2^{32}$ *with applications to MD5,* 71–80.

I. Biehl, J. Buchmann, B. Meyer, C. Thiel, C. Thiel, *Tools for proving 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 Heijst, *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,* 113–123.

J.D. Golić, S.V. Petrović, *A generalized correlation attack with a probabilistic constrained edit distance,* 472–476.

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,* 477–481.

K. Koyama, *Secure conference key distribution schemes for conspiracy attacks,* 449–453.

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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

Advances in Cryptology – **EUROCRYPT '93**, Lofthus, Norway. Springer-Verlag LNCS 765 (1994).
Editor: T. Helleseth.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

N. Ferguson, *Single term off-line coins,* 318–328.

R.A. Games, J.J. Rushanan, *Blind synchronization of m-sequences with even span,* 168–180.

R. Göttfert, H. Niederreiter, *On the linear complexity of products of shift-register sequences,* 151–158.

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,* 1–11.

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,* 305–317.

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,* 92–111.

E. Biham, *On Matsui's linear cryptanalysis,* 341–355.

E. Biham, A. Biryukov, *An improvement of Davies' attack on DES,* 461–467.

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,* 433–438.

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,* 306–319.

M. Franklin, M. Yung, *The blinding of weak signatures,* 67–76.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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,* 419–424.

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, O. 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. Seberry, X.-M. Zhang, Y. Zheng, *Relationships among nonlinearity criteria,* 376–388.

A. Shamir, *Memory efficient variants of public-key schemes for smart card applications,* 445–449.

P. Syverson, C. Meadows, *Formal requirements for key distribution protocols,* 320–331.

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 Micali'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,* 311–318.

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 of knowledge with preprocessing,* 413–416.

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. Micali, *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 of linear cryptanalysis and the applicability of Matsui'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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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* $y^2 + axy \equiv x^3 \pmod{n}$*,* 329–340.

H. Krawczyk, *New hash functions for message authentication,* 301–310.

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.

P.L. 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 cryptosystems,* 341–355.

C.P. Schnorr, H.H. Hörner, *Attacking the Chor-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 mod* p*,* 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. Blackburn, M. Burmester, Y. Desmedt, P. Wild, *Efficient multiplicative sharing schemes,* 107–118.

D. Bleichenbacher, *Generating ElGamal signatures without knowing the secret key,* 10–18.

J. Boyar, R. Peralta, *Short discreet proofs,* 131–142.

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. Stern, *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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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. Müller, *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 isomorphisms of polynomials (IP): Two new families of asymmetric algorithms,* 33–48.
B. Pfitzmann, M. Schunter, *Asymmetric fingerprinting,* 84–95.
D. Pointcheval, J. Stern, *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 modern 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,* 51–55.
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,* 185–190.
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 FFT-hashing,* 149–156.
D. Wheeler, *A bulk data encryption algorithm,* 127–134.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

Fast Software Encryption: Second International Workshop, Leuven, Belgium, December 1994.
Springer-Verlag LNCS 1008 (1995).
Editor: B. Preneel

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

Fast Software Encryption: Third International Workshop, Cambridge, UK., February 1996.
Springer-Verlag LNCS 1039 (1996).
Editor: D. Gollmann

©1997 CRC Press LLC

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-weight parity checks based on error-correcting codes,* 159–172.

V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, *The cipher SHARK,* 99-111.

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, 1988-1996)

M. Abadi, J. Feigenbaum, *Secure circuit evaluation,* 2 (1990), 1–12.

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, *Certifying permutations: 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.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

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), 1–25.

A. De Santis, G. Persiano, *The power of preprocessing in zero-knowledge proofs of knowledge,* 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, O. Goldreich, S. Micali, *On-line/off-line digital signatures,* 9 (1996), 35–67.

J.-H. Evertse, E. van Heijst, *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), 1–25.

O. Goldreich, *A uniform-complexity treatment of encryption and zero-knowledge,* 6 (1993), 21–53.

O. Goldreich, A. Kahan, *How to construct constant-round zero-knowledge proof systems for NP,* 9 (1996), 167–189.

O. Goldreich, E. Kushilevitz, *A perfect zero-knowledge proof system for a problem equivalent to the discrete logarithm,* 6 (1993), 97–116.

O. Goldreich, Y. Oren, *Definitions and properties of zero-knowledge proof systems,* 7 (1994), 1–32.

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 Levenshtein 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 of password security,* 1 (1989), 151–158.

S.S. Magliveras, N.D. Memon, *Algebraic properties of cryptosystem PGM,* 5 (1992), 167–183.

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC

Downloaded by [ETH BIBLIOTHEK (Zurich)] at 06:10 22 March 2017

©1997 CRC Press LLC