References

[1] M. Abadi and R. Needham, "Prudent engineering practice for cryptographic protocols", DEC SRC report #125, Digital Equipment Corporation, Palo Alto, CA, 1994.

[2] M. Abadi and M.R. Tuttle, "A semantics for a logic of authentication", *Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing*, 201–216, 1991.

[3] C. Adams, "Symmetric cryptographic system for data encryption", U.S. Patent # 5,511,123, 23 Apr 1996.

[4] ———, "IDUP and SPKM: Developing public-key-based APIs and mechanisms for communication security services", *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, 128–135, IEEE Computer Society Press, 1996.

[5] C. Adams and H. Meijer, "Security-related comments regarding McEliece's public-key cryptosystem", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 224–228, 1988.

[6] ———, "Security-related comments regarding McEliece's public-key cryptosystem", *IEEE Transactions on Information Theory*, 35 (1989), 454–455. An earlier version appeared in [5].

[7] C. Adams and S.E. Tavares, "Designing S-boxes for ciphers resistant to differential cryptanalysis", W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy*, 181–190, 1993.

[8] L.M. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography", *Proceedings of the IEEE 20th Annual Symposium on Foundations of Computer Science*, 55–60, 1979.

[9] ———, "The function field sieve", *Algorithmic Number Theory (LNCS 877)*, 108–121, 1994.

[10] ———, "Molecular computation of solutions to combinatorial problems", *Science*, 266 (1994), 1021–1024.

[11] L.M. Adleman and J. DeMarrais, "A subexponential algorithm for discrete logarithms over all finite fields", *Mathematics of Computation*, 61 (1993), 1–15.

[12] L.M. Adleman, J. DeMarrais, and M.-D. Huang, "A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields", *Algorithmic Number Theory (LNCS 877)*, 28–40, 1994.

[13] L.M. Adleman and M.-D. A. Huang, *Primality Testing and Abelian Varieties Over Finite Fields*, Springer-Verlag, Berlin, 1992.

[14] L.M. Adleman and H.W. Lenstra Jr., "Finding irreducible polynomials over finite fields", *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, 350–355, 1986.

[15] L.M. Adleman and K.S. McCurley, "Open problems in number theoretic complexity, II", *Algorithmic Number Theory (LNCS 877)*, 291–322, 1994.

[16] L.M. Adleman, C. Pomerance, and R.S. Rumely, "On distinguishing prime numbers from composite numbers", *Annals of Mathematics*, 117 (1983), 173–206.

[17] G.B. Agnew, "Random sources for cryptographic systems", *Advances in Cryptology–EUROCRYPT '87 (LNCS 304)*, 77–81, 1988.

[18] G.B. Agnew, R.C. Mullin, I.M. Onyszchuk, and S.A. Vanstone, "An implementation for a fast public-key cryptosystem", *Journal of Cryptology*, 3 (1991), 63–79.

[19] G.B. Agnew, R.C. Mullin, and S.A. Vanstone, "Improved digital signature scheme based on discrete exponentiation", *Electronics Letters*, 26 (July 5, 1990), 1024–1025.

[20] S.G. Akl, "On the security of compressed encodings", *Advances in Cryptology–Proceedings of Crypto 83*, 209–230, 1984.

[21] N. Alexandris, M. Burmester, V. Chrissikopoulos, and Y. Desmedt, "A secure key distribution system", W. Wolfowicz,

editor, *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy*, 30–34, Feb. 1993.

[22] W. ALEXI, B. CHOR, O. GOLDREICH, AND C.P. SCHNORR, "RSA/Rabin bits are $\frac{1}{2} + 1/poly(\log n)$ secure", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science*, 449–457, 1984.

[23] ———, "RSA and Rabin functions: Certain parts are as hard as the whole", *SIAM Journal on Computing*, 17 (1988), 194–209. An earlier version appeared in [22].

[24] W.R. ALFORD, A. GRANVILLE, AND C. POMERANCE, "There are infinitely many Carmichael numbers", *Annals of Mathematics*, 140 (1994), 703–722.

[25] H. AMIRAZIZI AND M. HELLMAN, "Time-memory-processor trade-offs", *IEEE Transactions on Information Theory*, 34 (1988), 505–512.

[26] R. ANDERSON, "Practical RSA trapdoor", *Electronics Letters*, 29 (May 27, 1993), 995.

[27] ———, "The classification of hash functions", P.G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, 83–93, Institute of Mathematics & Its Applications (IMA), 1995.

[28] ———, "On Fibonacci keystream generators", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 346–352, Springer-Verlag, 1995.

[29] ———, "Searching for the optimum correlation attack", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 137–143, Springer-Verlag, 1995.

[30] R. ANDERSON AND E. BIHAM, "Two practical and provably secure block ciphers: BEAR and LION", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 113–120, Springer-Verlag, 1996.

[31] R. ANDERSON AND R. NEEDHAM, "Robustness principles for public key protocols", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 236–247, 1995.

[32] N.C. ANKENY, "The least quadratic non residue", *Annals of Mathematics*, 55 (1952), 65–72.

[33] ANSI X3.92, "American National Standard – Data Encryption Algorithm", American National Standards Institute, 1981.

[34] ANSI X3.106, "American National Standard for Information Systems – Data Encryption Algorithm – Modes of Operation", American National Standards Institute, 1983.

[35] ANSI X9.8, "American National Standard for Financial Services – Banking – Personal Identification Number management and security. Part 1: PIN protection principles and techniques; Part 2: Approved algorithms for PIN encipherment", ASC X9 Secretariat – American Bankers Association, 1995.

[36] ANSI X9.9 (REVISED), "American National Standard – Financial institution message authentication (wholesale)", ASC X9 Secretariat – American Bankers Association, 1986 (replaces X9.9–1982).

[37] ANSI X9.17, "American National Standard – Financial institution key management (wholesale)", ASC X9 Secretariat – American Bankers Association, 1985.

[38] ANSI X9.19, "American National Standard – Financial institution retail message authentication", ASC X9 Secretariat – American Bankers Association, 1986.

[39] ANSI X9.23, "American National Standard – Financial institution encryption of wholesale financial messages", ASC X9 Secretariat – American Bankers Association, 1988.

[40] ANSI X9.24, "American National Standard for Financial Services – Financial services retail key management", ASC X9 Secretariat – American Bankers Association, 1992.

[41] ANSI X9.26, "American National Standard – Financial institution sign-on authentication for wholesale financial transactions", ASC X9 Secretariat – American Bankers Association, 1990.

[42] ANSI X9.28, "American National Standard for Financial Services – Financial institution multiple center key management (wholesale)", ASC X9 Secretariat – American Bankers Association, 1991.

[43] ANSI X9.30 (PART 1), "American National Standard for Financial Services – Public key cryptography using irreversible algorithms for the financial services industry – Part 1: The digital signature algorithm (DSA)", ASC X9 Secretariat – American Bankers Association, 1995.

[44] ANSI X9.30 (PART 2), "American National Standard for Financial Services – Public key cryptography using irreversible algorithms for the financial services industry – Part 2: The secure hash algorithm (SHA)", ASC X9 Secretariat – American Bankers Association, 1993.

[45] ANSI X9.31 (PART 1), "American National Standard for Financial Services – Public key cryptography using RSA for the financial services industry – Part 1: The RSA signature algorithm", draft, 1995.

[46] ANSI X9.31 (PART 2), "American National Standard for Financial Services – Public key cryptography using RSA for the financial services industry – Part 2: Hash algorithms for RSA", draft, 1995.

[47] ANSI X9.42, "Public key cryptography for the financial services industry: Management of symmetric algorithm keys using Diffie-Hellman", draft, 1995.

[48] ANSI X9.44, "Public key cryptography using reversible algorithms for the financial services industry: Transport of symmetric algorithm keys using RSA", draft, 1994.

[49] ANSI X9.45, "Public key cryptography for the financial services industry – Enhanced management controls using digital signatures and attribute certificates", draft, 1996.

[50] ANSI X9.52, "Triple data encryption algorithm modes of operation", draft, 1996.

[51] ANSI X9.55, "Public key cryptography for the financial services industry – Extensions to public key certificates and certificate revocation lists", draft, 1995.

[52] ANSI X9.57, "Public key cryptography for the financial services industry – Certificate management", draft, 1995.

[53] K. AOKI AND K. OHTA, "Differential-linear cryptanalysis of FEAL-8", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, E79-A (1996), 20–27.

[54] B. ARAZI, "Integrating a key distribution procedure into the digital signature standard", *Electronics Letters*, 29 (May 27, 1993), 966–967.

[55] ———, "On primality testing using purely divisionless operations", *The Computer Journal*, 37 (1994), 219–222.

[56] F. ARNAULT, "Rabin-Miller primality test: composite numbers which pass it", *Mathematics of Computation*, 64 (1995), 355–361.

[57] A.O.L. ATKIN AND R.G. LARSON, "On a primality test of Solovay and Strassen", *SIAM Journal on Computing*, 11 (1982), 789–791.

[58] A.O.L. ATKIN AND F. MORAIN, "Elliptic curves and primality proving", *Mathematics of Computation*, 61 (1993), 29–68.

[59] D. ATKINS, M. GRAFF, A.K. LENSTRA, AND P.C. LEYLAND, "The magic words are SQUEAMISH OSSIFRAGE", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 263–277, 1995.

[60] L. BABAI, "Trading group theory for randomness", *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, 421–429, 1985.

[61] L. BABAI AND S. MORAN, "Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes", *Journal of Computer and System Sciences*, 36 (1988), 254–276.

[62] E. BACH, "Discrete logarithms and factoring", Report No. UCB/CSD 84/186, Computer Science Division (EECS), University of California, Berkeley, California, 1984.

[63] ———, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, MIT Press, Cambridge, Massachusetts, 1985. An ACM Distinguished Dissertation.

[64] ———, "Explicit bounds for primality testing and related problems", *Mathematics of Computation*, 55 (1990), 355–380.

[65] ———, "Number-theoretic algorithms", *Annual Review of Computer Science*, 4 (1990), 119–172.

[66] ———, "Realistic analysis of some randomized algorithms", *Journal of Computer and System Sciences*, 42 (1991), 30–53.

[67] ———, "Toward a theory of Pollard's rho method", *Information and Computation*, 90 (1991), 139–155.

[68] E. BACH AND J. SHALLIT, "Factoring with cyclotomic polynomials", *Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science*, 443–450, 1985.

[69] ———, "Factoring with cyclotomic polynomials", *Mathematics of Computation*, 52 (1989), 201–219. An earlier version appeared in [68].

[70] ———, *Algorithmic Number Theory, Volume I: Efficient Algorithms*, MIT Press, Cambridge, Massachusetts, 1996.

[71] E. BACH AND J. SORENSON, "Sieve algorithms for perfect power testing", *Algorithmica*, 9 (1993), 313–328.

[72] A. BAHREMAN, "PEMToolKit: Building a top-down certification hierarchy", *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, 161–171, IEEE Computer Society Press, 1995.

[73] T. BARITAUD, M. CAMPANA, P. CHAUVAUD, AND H. GILBERT, "On the security of the permuted kernel identification scheme", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 305–311, 1993.

[74] W. BARKER, *Cryptanalysis of the Hagelin Cryptograph*, Aegean Park Press, Laguna Hills, California, 1977.

[75] P. BARRETT, "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 311–323, 1987.

[76] R.K. BAUER, T.A. BERSON, AND R.J. FEIERTAG, "A key distribution protocol using event markers", *ACM Transactions on Computer Systems*, 1 (1983), 249–255.

[77] U. BAUM AND S. BLACKBURN, "Clock-controlled pseudorandom generators on finite groups", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 6–21, Springer-Verlag, 1995.

[78] F. BAUSPIESS AND H.-J. KNOBLOCH, "How to keep authenticity alive in a computer network", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 38–46, 1990.

[79] D. BAYER, S. HABER, AND W.S. STORNETTA, "Improving the efficiency and reliability of digital time-stamping", R. Capocelli, A. De Santis, and U. Vaccaro, editors, *Sequences II: Methods in Communication, Security, and Computer Science*, 329–334, Springer-Verlag, 1993.

[80] P. BEAUCHEMIN AND G. BRASSARD, "A generalization of Hellman's extension to Shannon's approach to cryptography", *Journal of Cryptology*, 1 (1988), 129–131.

[81] P. BEAUCHEMIN, G. BRASSARD, C. CRÉPEAU, C. GOUTIER, AND C. POMERANCE, "The generation of random numbers that are probably prime", *Journal of Cryptology*, 1 (1988), 53–64.

[82] P. BÉGUIN AND J.-J. QUISQUATER, "Secure acceleration of DSS signatures using insecure server", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 249–259, 1995.

[83] A. BEIMEL AND B. CHOR, "Interaction in key distribution schemes", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 444–455, 1994.

[84] H. BEKER AND F. PIPER, *Cipher Systems: The Protection of Communications*, John Wiley & Sons, New York, 1982.

[85] H. BEKER AND M. WALKER, "Key management for secure electronic funds transfer in a retail environment", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 401–410, 1985.

[86] M. BELLARE, R. CANETTI, AND H. KRAWCZYK, "Keying hash functions for message authenticaion", *Advances in Cryptology–CRYPTO '96 (LNCS 1109)*, 1–15, 1996.

[87] M. BELLARE AND O. GOLDREICH, "On defining proofs of knowledge", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 390–420, 1993.

[88] M. BELLARE, O. GOLDREICH, AND S. GOLDWASSER, "Incremental cryptography: The case of hashing and signing", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 216–233, 1994.

[89] ———, "Incremental cryptography and application to virus protection", *Proceedings of the 27th Annual ACM Symposium on Theory of Computing*, 45–56, 1995.

[90] M. BELLARE, R. GUÉRIN, AND P. ROGAWAY, "XOR MACs: New methods for message authentication using finite pseudorandom functions", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 15–28, 1995.

[91] M. BELLARE, J. KILIAN, AND P. ROGAWAY, "The security of cipher block chaining", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 341–358, 1994.

[92] M. BELLARE AND S. MICALI, "How to sign given any trapdoor function", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 200–215, 1990.

[93] M. BELLARE AND P. ROGAWAY, "Random oracles are practical: a paradigm for designing efficient protocols", *1st ACM Conference on Computer and Communications Security*, 62–73, ACM Press, 1993.

[94] ———, "Entity authentication and key distribution", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 232–249, 1994.

[95] ———, "Optimal asymmetric encryption", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 92–111, 1995.

[96] ———, "Provably secure session key distribution – the three party case", *Proceedings of the 27th Annual ACM Symposium on Theory of Computing*, 57–66, 1995.

[97] M.J. BELLER, L.-F. CHANG, AND Y. YACOBI, "Privacy and authentication on a portable communications system", *IEEE Global Telecommunications Conference*, 1922–1927, 1991.

[98] ———, "Security for personal communications services: public-key vs. private key approaches", *The Third IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'92)*, 26–31, 1992.

[99] ———, "Privacy and authentication on a portable communications system", *IEEE Journal on Selected Areas in Communications*, 11 (1993), 821–829.

[100] M.J. BELLER AND Y. YACOBI, "Minimal asymmetric authentication and key agreement schemes", October 1994 unpublished manuscript.

[101] ———, "Fully-fledged two-way public key authentication and key agreement for low-cost terminals", *Electronics Letters*, 29 (May 27, 1993), 999–1001.

[102] S.M. BELLOVIN AND M. MERRITT, "Cryptographic protocol for secure communications", U.S. Patent # 5,241,599, 31 Aug 1993.

[103] ———, "Limitations of the Kerberos authentication system", *Computer Communication Review*, 20 (1990), 119–132.

[104] ———, "Encrypted key exchange: password-based protocols secure against dictionary attacks", *Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, 72–84, 1992.

[105] ———, "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise", *1st ACM Conference on Computer and Communications Security*, 244–250, ACM Press, 1993.

[106] ———, "An attack on the Interlock Protocol when used for authentication", *IEEE Transactions on Information Theory*, 40 (1994), 273–275.

[107] I. BEN-AROYA AND E. BIHAM, "Differential cyptanalysis of Lucifer", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 187–199, 1994.

[108] ———, "Differential cryptanalysis of Lucifer", *Journal of Cryptology*, 9 (1996), 21–34. An earlier version appeared in [107].

[109] M. BEN-OR, "Probabilistic algorithms in finite fields", *Proceedings of the IEEE 22nd Annual Symposium on Foundations of Computer Science*, 394–398, 1981.

[110] J. BENALOH, "Secret sharing homomorphisms: Keeping shares of a secret secret", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 251–260, 1987.

[111] J. BENALOH AND M. DE MARE, "One-way accumulators: A decentralized alternative to digital signatures", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 274–285, 1994.

[112] J. BENALOH AND J. LEICHTER, "Generalized secret sharing and monotone functions", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 27–35, 1990.

[113] S. BENGIO, G. BRASSARD, Y.G. DESMEDT, C. GOUTIER, AND J.-J. QUISQUATER, "Secure implementation of identification systems", *Journal of Cryptology*, 4 (1991), 175–183.

[114] C. BENNETT, G. BRASSARD, S. BREIDBART, AND S. WIESNER, "Quantum cryptography, or unforgeable subway tokens", *Advances in Cryptology–Proceedings of Crypto 82*, 267–275, 1983.

[115] C. BENNETT, G. BRASSARD, AND A. EKERT, "Quantum cryptography", *Scientific American*, special issue (1997), 164–171.

[116] S. BERKOVITS, "How to broadcast a secret", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 535–541, 1991.

[117] E.R. BERLEKAMP, "Factoring polynomials over finite fields", *Bell System Technical Journal*, 46 (1967), 1853–1859.

[118] ———, *Algebric Coding Theory*, McGraw Hill, New York, 1968.

[119] ———, "Factoring polynomials over large finite fields", *Mathematics of Computation*, 24 (1970), 713–735.

[120] E.R. BERLEKAMP, R.J. MCELIECE, AND H.C.A. VAN TILBORG, "On the inherent intractability of certain coding problems", *IEEE Transactions on Information Theory*, 24 (1978), 384–386.

[121] D.J. BERNSTEIN, "Detecting perfect powers in essentially linear time", preprint, 1995.

[122] D.J. BERNSTEIN AND A.K. LENSTRA, "A general number field sieve implementation", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, 103–126, Springer-Verlag, 1993.

[123] T. BETH, "Efficient zero-knowledge identification scheme for smart cards", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 77–84, 1988.

[124] T. BETH AND Z.-D. DAI, "On the complexity of pseudo-random sequences – or: If you can describe a sequence it can't be random", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 533–543, 1990.

[125] T. BETH, H.-J. KNOBLOCH, M. OTTEN, G.J. SIMMONS, AND P. WICHMANN, "Towards acceptable key escrow systems", *2nd ACM Conference on Computer and Communications Security*, 51–58, ACM Press, 1994.

[126] T. BETH AND F.C. PIPER, "The stop-and-go generator", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 88–92, 1985.

[127] J. BIERBRAUER, T. JOHANSSON, G. KABATIANSKII, AND B. SMEETS, "On families of hash functions via geometric codes and concatenation", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 331–342, 1994.

[128] E. BIHAM, "New types of cryptanalytic attacks using related keys", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 398–409, 1994.

[129] ———, "New types of cryptanalytic attacks using related keys", *Journal of Cryptology*, 7 (1994), 229–246. An earlier version appeared in [128].

[130] ———, "On modes of operation", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 116–120, Springer-Verlag, 1994.

[131] ———, "Cryptanalysis of multiple modes of operation", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 278–292, 1995.

[132] ———, "On Matsui's linear cryptanalysis", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 341–355, 1995.

[133] E. BIHAM AND A. BIRYUKOV, "How to strengthen DES using existing hardware", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 398–412, 1995.

[134] E. BIHAM AND A. SHAMIR, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology*, 4 (1991), 3–72. An earlier version appeared in [135].

[135] ———, "Differential cryptanalysis of DES-like cryptosystems", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 2–21, 1991.

[136] ———, "Differential cryptanalysis of Feal and N-Hash", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 1–16, 1991.

[137] ———, "Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI, and Lucifer", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 156–171, 1992.

[138] ———, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, New York, 1993.

[139] ———, "Differential cryptanalysis of the full 16-round DES", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 487–496, 1993.

[140] R. BIRD, I. GOPAL, A. HERZBERG, P. JANSON, S. KUTTEN, R. MOLVA, AND M. YUNG, "Systematic design of two-party authentication protocols", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 44–61, 1992.

[141] ———, "Systematic design of a family of attack-resistant authentication protocols", *IEEE Journal on Selected Areas in Communications*, 11 (1993), 679–693.

[142] ———, "The KryptoKnight family of lightweight protocols for authentication and key distribution", *IEEE/ACM Transactions on Networking*, 3 (1995), 31–41.

[143] S. BLACKBURN, S. MURPHY, AND J. STERN, "The cryptanalysis of a public-key implementation of finite group mappings", *Journal of Cryptology*, 8 (1995), 157–166.

[144] R.E. BLAHUT, *Principles and Practice of Information Theory*, Addison-Wesley, Reading, Massachusetts, 1987.

[145] I.F. BLAKE, R. FUJI-HARA, R.C. MULLIN, AND S.A. VANSTONE, "Computing logarithms in finite fields of characteristic two", *SIAM Journal on Algebraic and Discrete Methods*, 5 (1984), 276–285.

[146] I.F. BLAKE, S. GAO, AND R. LAMBERT, "Constructive problems for irreducible polynomials over finite fields", T.A. Gulliver and N.P. Secord, editors, *Information Theory and Applications (LNCS 793)*, 1–23, Springer-Verlag, 1994.

[147] B. BLAKLEY, G.R. BLAKLEY, A.H. CHAN, AND J.L. MASSEY, "Threshold schemes with disenrollment", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 540–548, 1993.

[148] G. BLAKLEY, "Safeguarding cryptographic keys", *Proceedings of AFIPS National Computer Conference*, 313–317, 1979.

[149] ———, "A computer algorithm for calculating the product AB modulo M", *IEEE Transactions on Computers*, 32 (1983), 497–500.

[150] G. BLAKLEY AND I. BOROSH, "Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages", *Computers and Mathematics with Applications*, 5:3 (1979), 169–178.

[151] G. BLAKLEY AND C. MEADOWS, "Security of ramp schemes", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 242–268, 1985.

[152] M. BLAZE, "Protocol failure in the escrowed encryption standard", *2nd ACM Conference on Computer and Communications Security*, 59–67, ACM Press, 1994.

[153] D. BLEICHENBACHER, "Generating ElGamal signatures without knowing the secret key", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 10–18, 1996.

[154] D. BLEICHENBACHER, W. BOSMA, AND A.K. LENSTRA, "Some remarks on Lucas-based cryptosystems", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 386–396, 1995.

[155] D. BLEICHENBACHER AND U. MAURER, "Directed acyclic graphs, one-way functions and digital signatures", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 75–82, 1994.

[156] U. BLÖCHER AND M. DICHTL, "Fish: A fast software stream cipher", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 41–44, Springer-Verlag, 1994.

[157] R. BLOM, "Non-public key distribution", *Advances in Cryptology–Proceedings of Crypto 82*, 231–236, 1983.

[158] ———, "An optimal class of symmetric key generation systems", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 335–338, 1985.

[159] L. BLUM, M. BLUM, AND M. SHUB, "Comparison of two pseudo-random number generators", *Advances in Cryptology–Proceedings of Crypto 82*, 61–78, 1983.

[160] ———, "A simple unpredictable pseudo-random number generator", *SIAM Journal on Computing*, 15 (1986), 364–383. An earlier version appeared in [159].

[161] M. BLUM, "Independent unbiased coin flips from a correlated biased source: a finite state Markov chain", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science*, 425–433, 1984.

[162] M. BLUM, A. DE SANTIS, S. MICALI, AND G. PERSIANO, "Noninteractive zero-knowledge", *SIAM Journal on Computing*, 20 (1991), 1084–1118.

[163] M. BLUM, P. FELDMAN, AND S. MICALI, "Non-interactive zero-knowledge and its applications", *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, 103–112, 1988.

[164] M. BLUM AND S. GOLDWASSER, "An efficient probabilistic public-key encryption scheme which hides all partial information", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 289–299, 1985.

[165] M. BLUM AND S. MICALI, "How to generate cryptographically strong sequences of pseudo random bits", *Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science*, 112–117, 1982.

[166] ———, "How to generate cryptographically strong sequences of pseudo-random bits",

SIAM Journal on Computing, 13 (1984), 850–864. An earlier version appeared in [165].

[167] C. BLUNDO AND A. CRESTI, "Space requirements for broadcast encryption", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 287–298, 1995.

[168] C. BLUNDO, A. CRESTI, A. DE SANTIS, AND U. VACCARO, "Fully dynamic secret sharing schemes", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 110–125, 1994.

[169] C. BLUNDO, A. DE SANTIS, A. HERZBERG, S. KUTTEN, U. VACCARO, AND M. YUNG, "Perfectly-secure key distribution for dynamic conferences", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 471–486, 1993.

[170] R.V. BOOK AND F. OTTO, "The verifiability of two-party protocols", *Advances in Cryptology–EUROCRYPT '85 (LNCS 219)*, 254–260, 1986.

[171] A. BOOTH, "A signed binary multiplication technique", *The Quarterly Journal of Mechanics and Applied Mathematics*, 4 (1951), 236–240.

[172] J. BOS AND D. CHAUM, "Provably unforgeable signatures", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 1–14, 1993.

[173] J. BOS AND M. COSTER, "Addition chain heuristics", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 400–407, 1990.

[174] W. BOSMA AND M.-P VAN DER HULST, "Faster primality testing", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 652–656, 1990.

[175] A. BOSSELAERS, R. GOVAERTS, AND J. VANDEWALLE, "Cryptography within phase I of the EEC-RACE programme", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 227–234, Springer-Verlag, 1993.

[176] ———, "Comparison of three modular reduction functions", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 175–186, 1994.

[177] ———, "Fast hashing on the Pentium", *Advances in Cryptology–CRYPTO '96 (LNCS 1109)*, 298–312, 1996.

[178] A. BOSSELAERS AND B. PRENEEL, editors, *Integrity Primitives for Secure Information Systems: Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040*, LNCS 1007, Springer-Verlag, New York, 1995.

[179] J. BOYAR, "Inferring sequences produced by a linear congruential generator missing low-order bits", *Journal of Cryptology*, 1 (1989), 177–184.

[180] ———, "Inferring sequences produced by pseudo-random number generators", *Journal of the Association for Computing Machinery*, 36 (1989), 129–141.

[181] J. BOYAR, D. CHAUM, I.B. DAMGÅRD, AND T. PEDERSEN, "Convertible undeniable signatures", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 189–205, 1991.

[182] C. BOYD, "Digital multisignatures", H. Beker and F. Piper, editors, *Cryptography and Coding*, Institute of Mathematics & Its Applications (IMA), 241–246, Clarendon Press, 1989.

[183] C. BOYD AND W. MAO, "On a limitation of BAN logic", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 240–247, 1994.

[184] B.O. BRACHTL, D. COPPERSMITH, M.M. HYDEN, S.M. MATYAS JR., C.H.W. MEYER, J. OSEAS, S. PILPEL, AND M. SCHILLING, "Data authentication using modification detection codes based on a public one-way encryption function", U.S. Patent # 4,908,861, 13 Mar 1990.

[185] S. BRANDS, "Restrictive blinding of secret-key certificates", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 231–247, 1995.

[186] J. BRANDT AND I. DAMGÅRD, "On generation of probable primes by incremental search", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 358–370, 1993.

[187] J. BRANDT, I. DAMGÅRD, AND P. LANDROCK, "Speeding up prime number generation", *Advances in Cryptology–ASIACRYPT '91 (LNCS 739)*, 440–449, 1993.

[188] J. BRANDT, I. DAMGÅRD, P. LANDROCK, AND T. PEDERSEN, "Zero-knowledge authentication scheme with secret key exchange", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 583–588, 1990.

[189] D.K. BRANSTAD, "Encryption protection in computer data communications", *Proceedings of the 4th Data Communications Symposium* (Quebec), 8.1–8.7, IEEE, 1975.

[190] G. BRASSARD, "A note on the complexity of cryptography", *IEEE Transactions on Information Theory*, 25 (1979), 232–233.

[191] ———, "On computationally secure authentication tags requiring short secret shared keys", *Advances in Cryptology–Proceedings of Crypto 82*, 79–86, 1983.

[192] ———, *Modern Cryptology: A Tutorial*, LNCS 325, Springer-Verlag, New York, 1988.

[193] G. BRASSARD, D. CHAUM, AND C. CRÉPEAU-, "Minimum disclosure proofs of knowledge", *Journal of Computer and System Sciences*, 37 (1988), 156–189.

[194] G. BRASSARD AND C. CRÉPEAU, "Zero-knowledge simulation of Boolean circuits", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 223–233, 1987.

[195] ———, "Sorting out zero-knowledge", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 181–191, 1990.

[196] R.P. BRENT, "An improved Monte Carlo factorization algorithm", *BIT*, 20 (1980), 176–184.

[197] R.P. BRENT AND J.M. POLLARD, "Factorization of the eighth Fermat number", *Mathematics of Computation*, 36 (1981), 627–630.

[198] D.M. BRESSOUD, *Factorization and Primality Testing*, Springer-Verlag, New York, 1989.

[199] E.F. BRICKELL, "A fast modular multiplication algorithm with applications to two key cryptography", *Advances in Cryptology–Proceedings of Crypto 82*, 51–60, 1983.

[200] ———, "Breaking iterated knapsacks", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 342–358, 1985.

[201] ———, "The cryptanalysis of knapsack cryptosystems", R.D. Ringeisen and F.S. Roberts, editors, *Applications of Discrete Mathematics*, 3–23, SIAM, 1988.

[202] E.F. BRICKELL AND J.M. DELAURENTIS, "An attack on a signature scheme proposed by Okamoto and Shiraishi", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 28–32, 1986.

[203] E.F. BRICKELL, D.M. GORDON, AND K.S. MCCURLEY, "Method for exponentiating in cryptographic systems", U.S. Patent # 5,299,262, 29 Mar 1994.

[204] E.F. BRICKELL, D.M. GORDON, K.S. MCCURLEY, AND D.B. WILSON, "Fast exponentiation with precomputation", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 200–207, 1993.

[205] E.F. BRICKELL, P.J. LEE, AND Y. YACOBI, "Secure audio teleconference", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 418–426, 1988.

[206] E.F. BRICKELL AND K.S. MCCURLEY, "An interactive identification scheme based on discrete logarithms and factoring", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 63–71, 1991.

[207] ———, "An interactive identification scheme based on discrete logarithms and factoring", *Journal of Cryptology*, 5 (1992), 29–39. An earlier version appeared in [206].

[208] E.F. BRICKELL AND A.M. ODLYZKO, "Cryptanalysis: A survey of recent results", *Proceedings of the IEEE*, 76 (1988), 578–593.

[209] ———, "Cryptanalysis: A survey of recent results", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 501–540, IEEE Press, 1992. An earlier version appeared in [208].

[210] J. BRILLHART, D. LEHMER, AND J. SELFRIDGE, "New primality criteria and factorizations of $2^m \pm 1$", *Mathematics of Computation*, 29 (1975), 620–647.

[211] J. BRILLHART, D. LEHMER, J. SELFRIDGE, B. TUCKERMAN, AND S. WAGSTAFF JR., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers*, volume 22 of *Contemporary Mathematics*, American Mathematical Society, Providence, Rhode Island, 2nd edition, 1988.

[212] J. BRILLHART AND J. SELFRIDGE, "Some factorizations of $2^n \pm 1$ and related results", *Mathematics of Computation*, 21 (1967), 87–96.

[213] D. BRILLINGER, *Time Series: Data Analysis and Theory*, Holden-Day, San Francisco, 1981.

[214] L. BROWN, M. KWAN, J. PIEPRZYK, AND J. SEBERRY, "Improving resistance to differential cryptanalysis and the redesign of LOKI", *Advances in Cryptology–ASIACRYPT '91 (LNCS 739)*, 36–50, 1993.

[215] L. BROWN, J. PIEPRZYK, AND J. SEBERRY, "LOKI – a cryptographic primitive for authentication and secrecy applications", *Advances*

in Cryptology–AUSCRYPT '90 (LNCS 453), 229–236, 1990.

[216] J. BUCHMANN AND S. DÜLLMANN, "On the computation of discrete logarithms in class groups", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 134–139, 1991.

[217] J. BUCHMANN, J. LOHO, AND J. ZAYER, "An implementation of the general number field sieve", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 159–165, 1994.

[218] J. BUCHMANN AND H.C. WILLIAMS, "A key-exchange system based on imaginary quadratic fields", *Journal of Cryptology*, 1 (1988), 107–118.

[219] J.P. BUHLER, H.W. LENSTRA JR., AND C. POMERANCE, "Factoring integers with the number field sieve", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, 50–94, Springer-Verlag, 1993.

[220] M. BURMESTER, "On the risk of opening distributed keys", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 308–317, 1994.

[221] M. BURMESTER AND Y. DESMEDT, "Remarks on soundness of proofs", *Electronics Letters*, 25 (October 26, 1989), 1509–1511.

[222] ———, "A secure and efficient conference key distribution system", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 275–286, 1995.

[223] M. BURMESTER, Y. DESMEDT, F. PIPER, AND M. WALKER, "A general zero-knowledge scheme", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 122–133, 1990.

[224] M. BURROWS, M. ABADI, AND R. NEEDHAM, "A logic of authentication", *Proceedings of the Royal Society of London Series A: Mathematical and Physical Sciences*, 246 (1989), 233–271. Preliminary version appeared as 1989 version of [227].

[225] ———, "A logic of authentication", *Proceedings of the 12th Annual ACM Symposium on Operating Systems Principles*, 1–13, 1989.

[226] ———, "A logic of authentication", *ACM Transactions on Computer Systems*, 8 (1990), 18–36.

[227] ———, "A logic of authentication", DEC SRC report #39, Digital Equipment Corporation, Palo Alto, CA, Feb. 1989. Revised Feb. 1990.

[228] J.L. CAMENISCH, J.-M. PIVETEAU, AND M.A. STADLER, "Blind signatures based on the discrete logarithm problem", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 428–432, 1995.

[229] K.W. CAMPBELL AND M.J. WIENER, "DES is not a group", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 512–520, 1993.

[230] C.M. CAMPBELL JR., "Design and specification of cryptographic capabilities", D.K. Branstad, editor, *Computer security and the Data Encryption Standard*, 54–66, NBS Special Publication 500-27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.

[231] E.R. CANFIELD, P. ERDÖS, AND C. POMERANCE, "On a problem of Oppenheim concerning 'Factorisatio Numerorum'", *Journal of Number Theory*, 17 (1983), 1–28.

[232] D.G. CANTOR AND H. ZASSENHAUS, "A new algorithm for factoring polynomials over finite fields", *Mathematics of Computation*, 36 (1981), 587–592.

[233] J.L. CARTER AND M.N. WEGMAN, "Universal classes of hash functions", *Proceedings of the 9th Annual ACM Symposium on Theory of Computing*, 106–112, 1977.

[234] ———, "Universal classes of hash functions", *Journal of Computer and System Sciences*, 18 (1979), 143–154. An earlier version appeared in [233].

[235] F. CHABAUD, "On the security of some cryptosystems based on error-correcting codes", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 131–139, 1995.

[236] G.J. CHAITIN, "On the length of programs for computing finite binary sequences", *Journal of the Association for Computing Machinery*, 13 (1966), 547–569.

[237] W.G. CHAMBERS, "Clock-controlled shift registers in binary sequence generators", *IEE Proceedings E – Computers and Digital Techniques*, 135 (1988), 17–24.

[238] ———, "Two stream ciphers", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 51–55, Springer-Verlag, 1994.

[239] W.G. CHAMBERS AND D. GOLLMANN, "Lock-in effect in cascades of clock-controlled shift-registers", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 331–343, 1988.

[240] B. CHAR, K. GEDDES, G. GONNET, B. LEONG, M. MONAGAN, AND S. WATT, *Maple V Library Reference Manual*, Springer-Verlag, New York, 1991.

[241] C. CHARNES, L. O'CONNOR, J. PIEPRZYK, R. SAFAVI-NAINI, AND Y. ZHENG, "Comments on Soviet encryption algorithm", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 433–438, 1995.

[242] D. CHAUM, "Blind signatures for untraceable payments", *Advances in Cryptology–Proceedings of Crypto 82*, 199–203, 1983.

[243] ———, "Security without identification: transaction systems to make big brother obsolete", *Communications of the ACM*, 28 (1985), 1030–1044.

[244] ———, "Demonstrating that a public predicate can be satisfied without revealing any information about how", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 195–199, 1987.

[245] ———, "Blinding for unanticipated signatures", *Advances in Cryptology–EUROCRYPT '87 (LNCS 304)*, 227–233, 1988.

[246] ———, "Zero-knowledge undeniable signatures", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 458–464, 1991.

[247] ———, "Designated confirmer signatures", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 86–91, 1995.

[248] D. CHAUM, J.-H. EVERTSE, AND J. VAN DE GRAAF, "An improved protocol for demonstrating possession of discrete logarithms and some generalizations", *Advances in Cryptology–EUROCRYPT '87 (LNCS 304)*, 127–141, 1988.

[249] D. CHAUM, J.-H. EVERTSE, J. VAN DE GRAAF, AND R. PERALTA, "Demonstrating possession of a discrete logarithm without revealing it", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 200–212, 1987.

[250] D. CHAUM, A. FIAT, AND M. NAOR, "Untraceable electronic cash", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 319–327, 1990.

[251] D. CHAUM AND T.P. PEDERSEN, "Wallet databases with observers", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 89–105, 1993.

[252] D. CHAUM AND H. VAN ANTWERPEN, "Undeniable signatures", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 212–216, 1990.

[253] D. CHAUM AND E. VAN HEIJST, "Group signatures", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 257–265, 1991.

[254] D. CHAUM, E. VAN HEIJST, AND B. PFITZMANN, "Cryptographically strong undeniable signatures, unconditionally secure for the signer", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 470–484, 1992.

[255] L. CHEN AND T.P. PEDERSEN, "New group signature schemes", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 171–181, 1995.

[256] V. CHEPYZHOV AND B. SMEETS, "On a fast correlation attack on certain stream ciphers", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 176–185, 1991.

[257] B. CHOR AND O. GOLDREICH, "Unbiased bits from sources of weak randomness and probabilistic communication complexity", *Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science*, 429–442, 1985.

[258] ———, "Unbiased bits from sources of weak randomness and probabilistic communication complexity", *SIAM Journal on Computing*, 17 (1988), 230–261. An earlier version appeared in [257].

[259] B. CHOR, S. GOLDWASSER, S. MICALI, AND B. AWERBUCH, "Verifiable secret sharing and achieving simultaneity in the presence of faults", *Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science*, 383–395, 1985.

[260] B. CHOR AND R.L. RIVEST, "A knapsack type public key cryptosystem based on arithmetic in finite fields", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 54–65, 1985.

[261] ———, "A knapsack-type public key cryptosystem based on arithmetic in finite fields", *IEEE Transactions on Information Theory*, 34 (1988), 901–909. An earlier version appeared in [260].

[262] A. CLARK, J. GOLIĆ, AND E. DAWSON, "A comparison of fast correlation attacks", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 145–157, Springer-Verlag, 1996.

[263] H. COHEN, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.

[264] H. COHEN AND A.K. LENSTRA, "Implementation of a new primality test", *Mathematics of Computation*, 48 (1987), 103–121.

[265] H. COHEN AND H.W. LENSTRA JR., "Primality testing and Jacobi sums", *Mathematics of Computation*, 42 (1984), 297–330.

[266] D. COPPERSMITH, "Fast evaluation of logarithms in fields of characteristic two", *IEEE Transactions on Information Theory*, 30 (1984), 587–594.

[267] ———, "Another birthday attack", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 14–17, 1986.

[268] ———, "The real reason for Rivest's phenomenon", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 535–536, 1986.

[269] ———, "Modifications to the number field sieve", *Journal of Cryptology*, 6 (1993), 169–180.

[270] ———, "Solving linear equations over $GF(2)$: Block Lanczos algorithm", *Linear Algebra and its Applications*, 192 (1993), 33–60.

[271] ———, "The Data Encryption Standard (DES) and its strength against attacks", *IBM Journal of Research and Development*, 38 (1994), 243–250.

[272] ———, "Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm", *Mathematics of Computation*, 62 (1994), 333–350.

[273] ———, "Finding a small root of a bivariate integer equation; factoring with high bits known", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 178–189, 1996.

[274] ———, "Finding a small root of a univariate modular equation", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 155–165, 1996.

[275] ———, "Analysis of ISO/CCITT Document X.509 Annex D", memorandum, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., June 11 1989.

[276] ———, "Two broken hash functions", IBM Research Report RC 18397, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Oct. 6 1992.

[277] D. COPPERSMITH, M. FRANKLIN, J. PATARIN, AND M. REITER, "Low-exponent RSA with related messages", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 1–9, 1996.

[278] D. COPPERSMITH, D.B. JOHNSON, AND S.M. MATYAS, "A proposed mode for triple-DES encryption", *IBM Journal of Research and Development*, 40 (1996), 253–261.

[279] D. COPPERSMITH, H. KRAWCZYK, AND Y. MANSOUR, "The shrinking generator", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 22–39, 1994.

[280] D. COPPERSMITH, A.M. ODLZYKO, AND R. SCHROEPPEL, "Discrete logarithms in $GF(p)$", *Algorithmica*, 1 (1986), 1–15.

[281] D. COPPERSMITH AND P. ROGAWAY, "Software-efficient pseudorandom function and the use thereof for encryption", U.S. Patent # 5,454,039, 26 Sep 1995.

[282] T.H. CORMEN, C.E. LEISERSON, AND R.L. RIVEST, *Introduction to Algorithms*, MIT Press, Cambridge, Massachusetts, 1990.

[283] M.J. COSTER, A. JOUX, B.A. LAMACCHIA, A.M. ODLYZKO, C.P. SCHNORR, AND J. STERN, "Improved low-density subset sum algorithms", *Computational Complexity*, 2 (1992), 111–128.

[284] J.-M. COUVEIGNES, "Computing a square root for the number field sieve", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, 95–102, Springer-Verlag, 1993.

[285] T. COVER AND R. KING, "A convergent gambling estimate of the entropy of English", *IEEE Transactions on Information Theory*, 24 (1978), 413–421.

[286] R.E. CRANDALL, "Method and apparatus for public key exchange in a cryptographic system", U.S. Patent # 5,159,632, 27 Oct 1992.

[287] ———, "Method and apparatus for public key exchange in a cryptographic system", U.S. Patent # 5,271,061, 14 Dec 1993 (continuation-in-part of 5,159,632).

[288] R.A. CROFT AND S.P. HARRIS, "Public-key cryptography and re-usable shared secrets", H. Beker and F. Piper, editors, *Cryptography and Coding*, Institute of Mathematics & Its Applications (IMA), 189–201, Clarendon Press, 1989.

[289] J. DAEMEN, *Cipher and hash function design*, PhD thesis, Katholieke Universiteit Leuven (Belgium), 1995.

[290] J. DAEMEN, R. GOVAERTS, AND J. VANDEWALLE, "A new approach to block cipher design", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 18–32, Springer-Verlag, 1994.

[291] ———, "Resynchronization weaknesses in synchronous stream ciphers", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 159–167, 1994.

[292] ———, "Weak keys for IDEA", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 224–231, 1994.

[293] Z.-D DAI, "Proof of Rueppel's linear complexity conjecture", *IEEE Transactions on Information Theory*, 32 (1986), 440–443.

[294] Z.-D. DAI AND J.-H. YANG, "Linear complexity of periodically repeated random sequences", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 168–175, 1991.

[295] I.B. DAMGÅRD, "Collision free hash functions and public key signature schemes", *Advances in Cryptology–EUROCRYPT '87 (LNCS 304)*, 203–216, 1988.

[296] ———, "A design principle for hash functions", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 416–427, 1990.

[297] ———, "Towards practical public key systems secure against chosen ciphertext attacks", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 445–456, 1992.

[298] ———, "Practical and provably secure release of a secret and exchange of signatures", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 200–217, 1994.

[299] I.B. DAMGÅRD AND P. LANDROCK, "Improved bounds for the Rabin primality test", M.J. Ganley, editor, *Cryptography and Coding III*, volume 45 of *Institute of Mathematics & Its Applications (IMA)*, 117–128, Clarendon Press, 1993.

[300] I.B. DAMGÅRD, P. LANDROCK, AND C. POMERANCE, "Average case error estimates for the strong probable prime test", *Mathematics of Computation*, 61 (1993), 177–194.

[301] H. DAVENPORT, "Bases for finite fields", *The Journal of the London Mathematical Society*, 43 (1968), 21–39.

[302] G.I. DAVIDA, "Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem", Technical Report TR-CS-82-2, Department of Electrical Engineering and Computer Science, University of Wisconsin, Milwaukee, WI, 1982.

[303] D.W. DAVIES, "Some regular properties of the 'Data Encryption Standard' algorithm", *Advances in Cryptology–Proceedings of Crypto 82*, 89–96, 1983.

[304] ———, "A message authenticator algorithm suitable for a mainframe computer", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 393–400, 1985.

[305] ———, "Schemes for electronic funds transfer at the point of sale", K.M. Jackson and J. Hruska, editors, *Computer Security Reference Book*, 667–689, CRC Press, 1992.

[306] D.W. DAVIES AND D.O. CLAYDEN, "The message authenticator algorithm (MAA) and its implementation", Report DITC 109/88, National Physical Laboratory, U.K., February 1988.

[307] D.W. DAVIES AND G.I.P. PARKIN, "The average cycle size of the key stream in output feedback encipherment", *Advances in Cryptology–Proceedings of Crypto 82*, 97–98, 1983.

[308] D.W. DAVIES AND W.L. PRICE, *Security for Computer Networks*, John Wiley & Sons, New York, 2nd edition, 1989.

[309] D. DAVIS, R. IHAKA, AND P. FENSTERMACHER, "Cryptographic randomness from air turbulence in disk drives", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 114–120, 1994.

[310] D. DAVIS AND R. SWICK, "Network security via private-key certificates", *Operating Systems Review*, 24 (1990), 64–67.

[311] J.A. DAVIS, D.B. HOLDRIDGE, AND G.J. SIMMONS, "Status report on factoring (at the Sandia National Labs)", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 183–215, 1985.

[312] E. DAWSON, "Cryptanalysis of summation generator", *Advances in Cryptology–AUSCRYPT '92 (LNCS 718)*, 209–215, 1993.

[313] W. DE JONGE AND D. CHAUM, "Attacks on some RSA signatures", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 18–27, 1986.

[314] P. DE ROOIJ, "On the security of the Schnorr scheme using preprocessing", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 71–80, 1991.

[315] ———, "On Schnorr's preprocessing for digital signature schemes", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 435–439, 1994.

[316] ———, "Efficient exponentiation using precomputation and vector addition chains", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 389–399, 1995.

[317] A. DE SANTIS, S. MICALI, AND G. PERSIANO, "Non-interactive zero-knowledge proof systems", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 52–72, 1988.

[318] A. DE SANTIS AND M. YUNG, "On the design of provably secure cryptographic hash functions", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 412–431, 1991.

[319] D. DE WALEFFE AND J.-J. QUISQUATER, "Better login protocols for computer networks", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 50–70, Springer-Verlag, 1993.

[320] J.M. DELAURENTIS, "A further weakness in the common modulus protocol for the RSA cryptoalgorithm", *Cryptologia*, 8 (1984), 253–259.

[321] N. DEMYTKO, "A new elliptic curve based analogue of RSA", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 40–49, 1994.

[322] B. DEN BOER, "Cryptanalysis of F.E.A.L.", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 293–299, 1988.

[323] ———, "Diffie-Hellman is as strong as discrete log for certain primes", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 530–539, 1990.

[324] B. DEN BOER AND A. BOSSELAERS, "An attack on the last two rounds of MD4", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 194–203, 1992.

[325] ———, "Collisions for the compression function of MD5", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 293–304, 1994.

[326] D.E. DENNING, *Cryptography and Data Security*, Addison-Wesley, Reading, Massachusetts, 1983. Reprinted with corrections.

[327] ———, "Digital signatures with RSA and other public-key cryptosystems", *Communications of the ACM*, 27 (1984), 388–392.

[328] ———, "To tap or not to tap", *Communications of the ACM*, 36 (1993), 24–44.

[329] D.E. DENNING AND D.K. BRANSTAD, "A taxonomy for key escrow encryption systems", *Communications of the ACM*, 39 (1996), 34–40.

[330] D.E. DENNING AND G.M. SACCO, "Timestamps in key distribution protocols", *Communications of the ACM*, 24 (1981), 533–536.

[331] D.E. DENNING AND M. SMID, "Key escrowing today", *IEEE Communications Magazine*, 32 (September 1994), 58–68.

[332] J. B. DENNIS AND E. C. VAN HORN, "Programming semantics for multiprogrammed computations", *Communications of the ACM*, 9 (1966), 143–155.

[333] T. DENNY, B. DODSON, A.K. LENSTRA, AND M.S. MANASSE, "On the factorization of RSA-120", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 166–174, 1994.

[334] DEPARTMENT OF DEFENSE (U.S.), "Department of defense password management guideline", CSC-STD-002-85, Department of Defense Computer Security Center, Fort Meade, Maryland, 1985.

[335] Y. DESMEDT, "Unconditionally secure authentication schemes and practical and theoretical consequences", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 42–55, 1986.

[336] ———, "Society and group oriented cryptography: A new concept", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 120–127, 1988.

[337] ———, "Threshold cryptography", *European Transactions on Telecommunications*, 5 (1994), 449–457.

[338] ———, "Securing traceability of ciphertexts – Towards a secure software key escrow system", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 147–157, 1995.

[339] Y. DESMEDT AND M. BURMESTER, "Towards practical 'proven secure' authenticated key distribution", *1st ACM Conference on Computer and Communications Security*, 228–231, ACM Press, 1993.

[340] Y. DESMEDT, C. GOUTIER, AND S. BENGIO, "Special uses and abuses of the Fiat-Shamir passport protocol", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 21–39, 1988.

[341] Y. DESMEDT AND A.M. ODLYZKO, "A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 516–522, 1986.

[342] W. DIFFIE, "The first ten years of public-key cryptography", *Proceedings of the IEEE*, 76 (1988), 560–577.

[343] ———, "The first ten years of public key cryptology", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 135–175, IEEE Press, 1992. An earlier version appeared in [342].

[344] W. DIFFIE AND M.E. HELLMAN, "Multiuser cryptographic techniques", *Proceedings of AFIPS National Computer Conference*, 109–112, 1976.

[345] ———, "New directions in cryptography", *IEEE Transactions on Information Theory*, 22 (1976), 644–654.

[346] ———, "Exhaustive cryptanalysis of the NBS Data Encryption Standard", *Computer*, 10 (1977), 74–84.

[347] ———, "Privacy and authentication: An introduction to cryptography", *Proceedings of the IEEE*, 67 (1979), 397–427.

[348] W. DIFFIE, P.C. VAN OORSCHOT, AND M.J. WIENER, "Authentication and authenticated key exchanges", *Designs, Codes and Cryptography*, 2 (1992), 107–125.

[349] C. DING, "The differential cryptanalysis and design of natural stream ciphers", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 101–115, Springer-Verlag, 1994.

[350] B. DIXON AND A.K. LENSTRA, "Massively parallel elliptic curve factoring", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 183–193, 1993.

[351] J.D. DIXON, "Asymptotically fast factorization of integers", *Mathematics of Computation*, 36 (1981), 255–260.

[352] H. DOBBERTIN, "Cryptanalysis of MD4", *Journal of Cryptology*, to appear.

[353] ———, "RIPEMD with two-round compress function is not collision-free", *Journal of Cryptology*, to appear; announced at rump session, Eurocrypt '95.

[354] ———, "Cryptanalysis of MD4", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 53–69, Springer-Verlag, 1996.

[355] H. DOBBERTIN, A. BOSSELAERS, AND B. PRENEEL, "RIPEMD-160: a strengthened version of RIPEMD", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 71–82, Springer-Verlag, 1996.

[356] B. DODSON AND A.K. LENSTRA, "NFS with four large primes: An explosive experiment", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 372–385, 1995.

[357] D. DOLEV, C. DWORK, AND M. NAOR, "Non-malleable cryptography", *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, 542–552, 1991.

[358] D. DOLEV AND A.C. YAO, "On the security of public key protocols", *Proceedings of the IEEE 22nd Annual Symposium on Foundations of Computer Science*, 350–357, 1981.

[359] ———, "On the security of public key protocols", *IEEE Transactions on Information Theory*, 29 (1983), 198–208. An earlier version appeared in [358].

[360] P. DOWNEY, B. LEONG, AND R. SETHI, "Computing sequences with addition chains", *SIAM Journal on Computing*, 10 (1981), 638–646.

[361] S.R. DUSSÉ AND B.S. KALISKI JR., "A cryptographic library for the Motorola DSP 56000", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 230–244, 1991.

[362] H. EBERLE, "A high-speed DES implementation for network applications", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 521–539, 1993.

[363] W. F. EHRSAM, C.H.W. MEYER, R.L. POWERS, J.L. SMITH, AND W.L. TUCHMAN, "Product block cipher system for data security", U.S. Patent # 3,962,539, 8 Jun 1976.

[364] W.F. EHRSAM, S.M. MATYAS, C.H. MEYER, AND W.L. TUCHMAN, "A cryptographic key management scheme for implementing the Data Encryption Standard", *IBM Systems Journal*, 17 (1978), 106–125.

[365] ELECTRONIC INDUSTRIES ASSOCIATION (EIA), "Dual-mode mobile station – base station compatibility standard", EIA Interim Standard IS-54 Revision B (Rev. B), 1992.

[366] T. ELGAMAL, *Cryptography and logarithms over finite fields*, PhD thesis, Stanford University, 1984.

[367] ———, "A public key cryptosystem and a signature scheme based on discrete logarithms", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 10–18, 1985.

[368] ———, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, 31 (1985), 469–472. An earlier version appeared in [367].

[369] ———, "A subexponential-time algorithm for computing discrete logarithms over GF(p^2)", *IEEE Transactions on Information Theory*, 31 (1985), 473–481.

[370] P. ELIAS, "The efficient construction of an unbiased random sequence", *The Annals of Mathematical Statistics*, 43 (1972), 865–870.

[371] ———, "Interval and recency rank source encoding: Two on-line adaptive variable-length schemes", *IEEE Transactions on Information Theory*, 33 (1987), 3–10.

[372] E.D. ERDMANN, "Empirical tests of binary keystreams", Master's thesis, Department of Mathematics, Royal Holloway and Bedford New College, University of London, 1992.

[373] P. ERDÖS AND C. POMERANCE, "On the number of false witnesses for a composite number", *Mathematics of Computation*, 46 (1986), 259–279.

[374] D. ESTES, L.M. ADLEMAN, K. KOMPELLA, K.S. MCCURLEY, AND G.L. MILLER, "Breaking the Ong-Schnorr-Shamir signature scheme for quadratic number fields", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 3–13, 1986.

[375] A. EVANS JR., W. KANTROWITZ, AND E. WEISS, "A user authentication scheme not requiring secrecy in the computer", *Communications of the ACM*, 17 (1974), 437–442.

[376] S. EVEN AND O. GOLDREICH, "On the power of cascade ciphers", *ACM Transactions on Computer Systems*, 3 (1985), 108–116.

[377] S. EVEN, O. GOLDREICH, AND S. MICALI, "On-line/off-line digital signatures", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 263–275, 1990.

[378] ———, "On-line/off-line digital signatures", *Journal of Cryptology*, 9 (1996), 35–67. An earlier version appeared in [377].

[379] S. EVEN AND Y. YACOBI, "Cryptocomplexity and NP-completeness", J.W. de Bakker and J. van Leeuwen, editors, *Automata, Languages, and Programming, 7th Colloquium (LNCS 85)*, 195–207, Springer-Verlag, 1980.

[380] D. EVERETT, "Identity verification and biometrics", K.M. Jackson and J. Hruska, editors, *Computer Security Reference Book*, 37–73, CRC Press, 1992.

[381] J.-H. EVERTSE AND E. VAN HEIJST, "Which new RSA-signatures can be computed from certain given RSA-signatures?", *Journal of Cryptology*, 5 (1992), 41–52.

[382] R.C. FAIRFIELD, R.L. MORTENSON, AND K.B. COULTHART, "An LSI random number generator (RNG)", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 203–230, 1985.

[383] U. FEIGE, A. FIAT, AND A. SHAMIR, "Zero-knowledge proofs of identity", *Journal of Cryptology*, 1 (1988), 77–94.

[384] U. FEIGE AND A. SHAMIR, "Witness indistinguishable and witness hiding protocols", *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, 416–426, 1990.

[385] H. FEISTEL, "Block cipher cryptographic system", U.S. Patent # 3,798,359, 19 Mar 1974.

[386] ———, "Step code ciphering system", U.S. Patent # 3,798,360, 19 Mar 1974.

[387] ———, "Cryptography and computer privacy", *Scientific American*, 228 (May 1973), 15–23.

[388] H. FEISTEL, W.A. NOTZ, AND J.L. SMITH, "Some cryptographic techniques for machine-to-machine data communications", *Proceedings of the IEEE*, 63 (1975), 1545–1554.

[389] F.A. FELDMAN, "Fast spectral tests for measuring nonrandomness and the DES", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 243–254, 1988.

[390] P. FELDMAN, "A practical scheme for non-interactive verifiable secret sharing", *Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science*, 427–437, 1987.

[391] D.C. FELDMEIER AND P.R. KARN, "UNIX password security – ten years later", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 44–63, 1990.

[392] W. FELLER, *An Introduction to Probability Theory and its Applications*, John Wiley & Sons, New York, 3rd edition, 1968.

[393] A. FIAT AND M. NAOR, "Rigorous time/space tradeoffs for inverting functions", *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, 534–541, 1991.

[394] ———, "Broadcast encryption", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 480–491, 1994.

[395] A. FIAT AND A. SHAMIR, "How to prove yourself: Practical solutions to identification and signature problems", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 186–194, 1987.

[396] FIPS 46, "Data encryption standard", Federal Information Processing Standards Publication 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977 (revised as FIPS 46-1:1988; FIPS 46-2:1993).

[397] FIPS 74, "Guidelines for implementing and using the NBS data encryption standard", Federal Information Processing Standards Publication 74, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1981.

[398] FIPS 81, "DES modes of operation", Federal Information Processing Standards Publication 81, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1980.

[399] FIPS 112, "Password usage", Federal Information Processing Standards Publication 112, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1985.

[400] FIPS 113, "Computer data authentication", Federal Information Processing Standards Publication 113, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1985.

[401] FIPS 140-1, "Security requirements for cryptographic modules", Federal Information Processing Standards Publication 140-1, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.

[402] FIPS 171, "Key management using ANSI X9.17", Federal Information Processing Standards Publication 171, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1992.

[403] FIPS 180, "Secure hash standard", Federal Information Processing Standards Publication 180, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, May 11 1993.

[404] FIPS 180-1, "Secure hash standard", Federal Information Processing Standards Publication 180-1, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, April 17 1995 (supersedes FIPS PUB 180).

[405] FIPS 185, "Escrowed encryption standard (EES)", Federal Information Processing Standards Publication 185, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.

[406] FIPS 186, "Digital signature standard", Federal Information Processing Standards Publication 186, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.

[407] FIPS 196, "Entity authentication using public key cryptography", U.S. Department of Commerce/N.I.S.T., February 18 1997.

[408] A.M. FISCHER, "Public key/signature cryptosystem with enhanced digital signature certification", U.S. Patent # 4,868,877, 19 Sep 1989.

[409] ———, "Public key/signature cryptosystem with enhanced digital signature certification", U.S. Patent # 5,005,200, 2 Apr 1991 (continuation-in-part of 4,868,877).

[410] ———, "Electronic document authorization", *Proceedings of the 13th National Computer*

Security Conference, Washington D.C., sponsored by N.I.S.T. and the National Computer Security Center, USA, 1990.

[411] J.-B. FISCHER AND J. STERN, "An efficient pseudo-random generator provably as secure as syndrome decoding", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 245–255, 1996.

[412] M. FISCHER, S. MICALI, AND C. RACKOFF, "A secure protocol for oblivious transfer", unpublished (presented at Eurocrypt'84).

[413] P. FLAJOLET AND A. ODLYZKO, "Random mapping statistics", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 329–354, 1990.

[414] W. FORD, *Computer Communications Security: Principles, Standard Protocols and Techniques*, Prentice Hall, Englewood Cliffs, New Jersey, 1994.

[415] ———, "Standardizing information technology security", *StandardView*, 2 (1994), 64–71.

[416] ———, "Advances in public-key certificate standards", *Security, Audit and Control*, 13 (1995), ACM Press/SIGSAC, 9–15.

[417] W. FORD AND M. WIENER, "A key distribution method for object-based protection", *2nd ACM Conference on Computer and Communications Security*, 193–197, ACM Press, 1994.

[418] R. FORRÉ, "A fast correlation attack on nonlinearly feedforward filtered shift-register sequences", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 586–595, 1990.

[419] Y. FRANKEL AND M. YUNG, "Cryptanalysis of the immunized LL public key systems", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 287–296, 1995.

[420] ———, "Escrow encryption systems visited: Attacks, analysis and designs", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 222–235, 1995.

[421] M.K. FRANKLIN AND M.K. REITER, "Verifiable signature sharing", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 50–63, 1995.

[422] G. FREY AND H.-G. RÜCK, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, 62 (1994), 865–874.

[423] W. FRIEDMAN, *Military Cryptanalysis*, U.S. Government Printing Office, Washington DC, 1944. Volume I – Monoalphabetic substitution systems. Volume II – Simpler varieties of polyalphabetic substitution systems. Volume III – Aperiodic substitutions. Volume IV – Transposition systems.

[424] ———, "Cryptology", *Encyclopedia Brittanica*, 6 (1967), 844–851.

[425] ———, *Elements of Cryptanalysis*, Aegean Park Press, Laguna Hills, California, 1976. First published in 1923.

[426] ———, *The Index of Coincidence and its Applications in Cryptography*, Aegean Park Press, Laguna Hills, California, 1979. First published in 1920.

[427] A.M. FRIEZE, J. HÅSTAD, R. KANNAN, J.C. LAGARIAS, AND A. SHAMIR, "Reconstructing truncated integer variables satisfying linear congruences", *SIAM Journal on Computing*, 17 (1988), 262–280.

[428] A. FUJIOKA, T. OKAMOTO, AND S. MIYAGUCHI, "ESIGN: An efficient digital signature implementation for smart cards", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 446–457, 1991.

[429] W. FUMY AND P. LANDROCK, "Principles of key management", *IEEE Journal on Selected Areas in Communications*, 11 (1993), 785–793.

[430] W. FUMY AND M. LECLERC, "Placement of cryptographic key distribution within OSI: design alternatives and assessment", *Computer Networks and ISDN Systems*, 26 (1993), 217–225.

[431] W. FUMY AND M. MUNZERT, "A modular approach to key distribution", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 274–283, 1991.

[432] W. FUMY AND M. RIETENSPIESS, "Open systems security standards", A. Kent and J.G. Williams, editors, *Encyclopedia of Computer Science and Technology 34*, 301–334, Marcel Dekker, 1996.

[433] K. GAARDER AND E. SNEKKENES, "Applying a formal analysis technique to the CCITT X.509 strong two-way authentication protocol", *Journal of Cryptology*, 3 (1991), 81–98.

[434] E.M. GABIDULIN, "On public-key cryptosystems based on linear codes: Efficiency and weakness", P.G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, 17–31, Institute of Mathematics & Its Applications (IMA), 1995.

[435] E.M. GABIDULIN, A.V. PARAMONOV, AND O.V. TRETJAKOV, "Ideals over a non-commutative ring and their application in cryptology", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 482–489, 1991.

[436] H. GAINES, *Cryptanalysis: A Study of Ciphers and their Solutions*, Dover Publications, New York, 1956.

[437] J. GAIT, "A new nonlinear pseudorandom number generator", *IEEE Transactions on Software Engineering*, 3 (1977), 359–363.

[438] J.M. GALVIN, K. MCCLOGHRIE, AND J.R. DAVIN, "Secure management of SNMP networks", *Integrated Network Management, II*, 703–714, 1991.

[439] R.A. GAMES AND A.H. CHAN, "A fast algorithm for determining the complexity of a binary sequence with period 2^n", *IEEE Transactions on Information Theory*, 29 (1983), 144–146.

[440] M. GARDNER, "A new kind of cipher that would take millions of years to break", *Scientific American*, 237 (Aug 1977), 120–124.

[441] M.R. GAREY AND D.S. JOHNSON, *Computers and Intractability: A Guide to the Theory of NP-completeness*, W.H. Freeman, San Francisco, 1979.

[442] S. GARFINKEL, *PGP: Pretty Good Privacy*, O'Reilly and Associates, Inc., Sebastopol, California, 1995.

[443] H. GARNER, "The residue number system", *IRE Transactions on Electronic Computers*, EC-8 (1959), 140–147.

[444] C.F. GAUSS, *Disquisitiones Arithmeticae*, 1801. English translation by Arthur A. Clarke, Springer-Verlag, New York, 1986.

[445] K. GEDDES, S. CZAPOR, AND G. LABAHN, *Algorithms for Computer Algebra*, Kluwer Academic Publishers, Boston, 1992.

[446] P. GEFFE, "How to protect data with ciphers that are really hard to break", *Electronics*, 46 (1973), 99–101.

[447] J. GEORGIADES, "Some remarks on the security of the identification scheme based on permuted kernels", *Journal of Cryptology*, 5 (1992), 133–137.

[448] J. GERVER, "Factoring large numbers with a quadratic sieve", *Mathematics of Computation*, 41 (1983), 287–294.

[449] P.J. GIBLIN, *Primes and Programming: An Introduction to Number Theory with Computing*, Cambridge University Press, Cambrige, 1993.

[450] J.K. GIBSON, "Some comments on Damgård's hashing principle", *Electronics Letters*, 26 (July 19, 1990), 1178–1179.

[451] ———, "Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 517–521, 1991.

[452] ———, "Severely denting the Gabidulin version of the McEliece public key cryptosystem", *Designs, Codes and Cryptography*, 6 (1995), 37–45.

[453] ———, "The security of the Gabidulin public key cryptosystem", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 212–223, 1996.

[454] E.N. GILBERT, F.J. MACWILLIAMS, AND N.J.A. SLOANE, "Codes which detect deception", *Bell System Technical Journal*, 53 (1974), 405–424.

[455] H. GILBERT AND G. CHASSÉ, "A statistical attack of the Feal-8 cryptosystem", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 22–33, 1991.

[456] H. GILBERT AND P. CHAUVAUD, "A chosen plaintext attack of the 16-round Khufu cryptosystem", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 359–368, 1994.

[457] M. GIRAULT, "Hash-functions using modulo-n operations", *Advances in Cryptology–EUROCRYPT '87 (LNCS 304)*, 217–226, 1988.

[458] ———, "An identity-based identification scheme based on discrete logarithms modulo a composite number", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 481–486, 1991.

[459] ———, "Self-certified public keys", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 490–497, 1991.

[460] M. GIRAULT, R. COHEN, AND M. CAMPANA, "A generalized birthday attack", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 129–156, 1988.

[461] M. GIRAULT AND J.C. PAILLÈS, "An identity-based scheme providing zero-knowledge authentication and authenticated key-exchange", *First European Symposium on Research in Computer Security – ESORICS'90*, 173–184, 1990.

[462] M. GIRAULT AND J. STERN, "On the length of cryptographic hash-values used in identification schemes", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 202–215, 1994.

[463] V.D. GLIGOR, R. KAILAR, S. STUBBLEBINE, AND L. GONG, "Logics for cryptographic protocols — virtues and limitations", *The Computer Security Foundations Workshop IV*, 219–226, IEEE Computer Security Press, 1991.

[464] C.M. GOLDIE AND R.G.E. PINCH, *Communication Theory*, Cambridge University Press, Cambridge, 1991.

[465] O. GOLDREICH, "Two remarks concerning the Goldwasser-Micali-Rivest signature scheme", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 104–110, 1987.

[466] O. GOLDREICH, S. GOLDWASSER, AND S. MICALI, "How to construct random functions", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science*, 464–479, 1984.

[467] ———, "On the cryptographic applications of random functions", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 276–288, 1985.

[468] ———, "How to construct random functions", *Journal of the Association for Computing Machinery*, 33 (1986), 792–807. An earlier version appeared in [466].

[469] O. GOLDREICH AND H. KRAWCZYK, "On the composition of zero-knowledge proof systems", M.S. Paterson, editor, *Automata, Languages and Programming, 17th International Colloquium (LNCS 443)*, 268–282, Springer-Verlag, 1990.

[470] O. GOLDREICH, H. KRAWCZYK, AND M. LUBY, "On the existence of pseudorandom generators", *Proceedings of the IEEE 29th Annual Symposium on Foundations of Computer Science*, 12–24, 1988.

[471] O. GOLDREICH AND L.A. LEVIN, "A hard-core predicate for all one-way functions", *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, 25–32, 1989.

[472] O. GOLDREICH, S. MICALI, AND A. WIGDERSON, "Proofs that yield nothing but their validity and a methodology of cryptographic protocol design", *Proceedings of the IEEE 27th Annual Symposium on Foundations of Computer Science*, 174–187, 1986.

[473] ———, "How to prove all NP statements in zero-knowledge, and a methodology of cryptographic protocol design", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 171–185, 1987.

[474] ———, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems", *Journal of the Association for Computing Machinery*, 38 (1991), 691–729. An earlier version appeared in [472].

[475] O. GOLDREICH AND Y. OREN, "Definitions and properties of zero-knowledge proof systems", *Journal of Cryptology*, 7 (1994), 1–32.

[476] S. GOLDWASSER, "The search for provably secure cryptosystems", C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, 89–113, American Mathematical Society, 1990.

[477] S. GOLDWASSER AND J. KILIAN, "Almost all primes can be quickly certified", *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, 316–329, 1986.

[478] S. GOLDWASSER AND S. MICALI, "Probabilistic encryption & how to play mental poker keeping secret all partial information", *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, 365–377, 1982.

[479] ———, "Probabilistic encryption", *Journal of Computer and System Sciences*, 28 (1984), 270–299. An earlier version appeared in [478].

[480] S. GOLDWASSER, S. MICALI, AND C. RACKOFF, "The knowledge complexity of interactive proof-systems", *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, 291–304, 1985.

[481] ———, "The knowledge complexity of interactive proof systems", *SIAM Journal on Computing*, 18 (1989), 186–208. An earlier version appeared in [480].

[482] S. GOLDWASSER, S. MICALI, AND R.L. RIVEST, "A "paradoxical" solution to the signature problem", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science*, 441–448, 1984.

[483] ———, "A "paradoxical" solution to the signature problem", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 467, 1985.

[484] ———, "A digital signature scheme secure against adaptive chosen-message attacks", *SIAM Journal on Computing*, 17 (1988), 281–308. Earlier versions appeared in [482] and [483].

[485] J. GOLIĆ, "Correlation via linear sequential circuit approximation of combiners with memory", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 113–123, 1993.

[486] ———, "On the security of shift register based keystream generators", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 90–100, Springer-Verlag, 1994.

[487] ———, "Intrinsic statistical weakness of keystream generators", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 91–103, 1995.

[488] ———, "Linear cryptanalysis of stream ciphers", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 154–169, Springer-Verlag, 1995.

[489] ———, "Towards fast correlation attacks on irregularly clocked shift registers", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 248–262, 1995.

[490] ———, "On the security of nonlinear filter generators", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 173–188, Springer-Verlag, 1996.

[491] J. GOLIĆ AND M. MIHALJEVIĆ, "A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance", *Journal of Cryptology*, 3 (1991), 201–212.

[492] J. GOLIĆ AND L. O'CONNOR, "Embedding and probabilistic correlation attacks on clock-controlled shift registers", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 230–243, 1995.

[493] R.A. GOLLIVER, A.K. LENSTRA, AND K.S. MCCURLEY, "Lattice sieving and trial division", *Algorithmic Number Theory (LNCS 877)*, 18–27, 1994.

[494] D. GOLLMANN, "Pseudo random properties of cascade connections of clock controlled shift registers", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 93–98, 1985.

[495] ———, "Cryptanalysis of clock controlled shift registers", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 121–126, Springer-Verlag, 1994.

[496] D. GOLLMANN AND W.G. CHAMBERS, "Clock-controlled shift registers: a review", *IEEE Journal on Selected Areas in Communications*, 7 (1989), 525–533.

[497] D. GOLLMANN, Y. HAN, AND C. MITCHELL, "Redundant integer representations and fast exponentiation", *Designs, Codes and Cryptography*, 7 (1996), 135–151.

[498] S.W. GOLOMB, *Shift Register Sequences*, Holden-Day, San Francisco, 1967. Reprinted by Aegean Park Press, 1982.

[499] L. GONG, "Using one-way functions for authentication", *Computer Communication Review*, 19 (1989), 8–11.

[500] ———, "A security risk of depending on synchronized clocks", *Operating Systems Review*, 26 (1992), 49–53.

[501] ———, "Variations on the themes of message freshness and replay", *The Computer Security Foundations Workshop VI*, 131–136, IEEE Computer Society Press, 1993.

[502] ———, "New protocols for third-party-based authentication and secure broadcast", *2nd ACM Conference on Computer and Communications Security*, 176–183, ACM Press, 1994.

[503] ———, "Efficient network authentication protocols: lower bounds and optimal implementations", *Distributed Computing*, 9 (1995), 131–145.

[504] L. GONG, T.M.A. LOMAS, R.M. NEEDHAM, AND J.H. SALTZER, "Protecting poorly chosen secrets from guessing attacks", *IEEE Journal on Selected Areas in Communications*, 11 (1993), 648–656.

[505] L. GONG, R. NEEDHAM, AND R. YAHALOM, "Reasoning about belief in cryptographic protocols", *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 234–248, 1990.

[506] L. GONG AND D.J. WHEELER, "A matrix key-distribution scheme", *Journal of Cryptology*, 2 (1990), 51–59.

[507] I.J. GOOD, "The serial test for sampling numbers and other tests for randomness", *Proceedings of the Cambridge Philosophical Society*, 49 (1953), 276–284.

[508] ———, "On the serial test for random sequences", *The Annals of Mathematical Statistics*, 28 (1957), 262–264.

[509] D.M. GORDON, "Designing and detecting trapdoors for discrete log cryptosystems", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 66–75, 1993.

[510] ———, "Discrete logarithms in GF(p) using the number field sieve", *SIAM Journal on Discrete Mathematics*, 6 (1993), 124–138.

[511] D.M. GORDON AND K.S. MCCURLEY, "Massively parallel computations of discrete logarithms", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 312–323, 1993.

[512] J. GORDON, "Very simple method to find the minimum polynomial of an arbitrary nonzero element of a finite field", *Electronics Letters*, 12 (December 9, 1976), 663–664.

[513] ———, "Strong RSA keys", *Electronics Letters*, 20 (June 7, 1984), 514–516.

[514] ———, "Strong primes are easy to find", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 216–223, 1985.

[515] ———, "How to forge RSA key certificates", *Electronics Letters*, 21 (April 25, 1985), 377–379.

[516] ———, "Fast multiplicative inverse in modular arithmetic", H. Beker and F. Piper, editors, *Cryptography and Coding*, Institute of Mathematics & Its Applications (IMA), 269–279, Clarendon Press, 1989.

[517] J. GORDON AND H. RETKIN, "Are big S-boxes best?", *Cryptography–Proceedings of the Workshop on Cryptography, Burg Feuerstein (LNCS 149)*, 257–262, 1983.

[518] M. GORESKY AND A. KLAPPER, "Feedback registers based on ramified extensions of the 2-adic numbers", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 215–222, 1995.

[519] K.C. GOSS, "Cryptographic method and apparatus for public key exchange with authentication", U.S. Patent # 4,956,863, 11 Sep 1990.

[520] R. GRAHAM, D. KNUTH, AND O. PATASHNIK, *Concrete Mathematics*, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1994.

[521] A. GRANVILLE, "Primality testing and Carmichael numbers", *Notices of the American Mathematical Society*, 39 (1992), 696–700.

[522] E. GROSSMAN, "Group theoretic remarks on cryptographic systems based on two types of addition", IBM Research Report RC 4742, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Feb. 26 1974.

[523] L.C. GUILLOU AND J.-J. QUISQUATER, "Method and apparatus for authenticating accreditations and for authenticating and signing messages", U.S. Patent # 5,140,634, 18 Aug 1992.

[524] ———, "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 123–128, 1988.

[525] L.C. GUILLOU, J.-J. QUISQUATER, M. WALKER, P. LANDROCK, AND C. SHAER, "Precautions taken against various potential attacks in ISO/IEC DIS 9796", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 465–473, 1991.

[526] L.C. GUILLOU AND M. UGON, "Smart card – a highly reliable and portable security device", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 464–479, 1987.

[527] L.C. GUILLOU, M. UGON, AND J.-J. QUISQUATER, "The smart card: A standardized security device dedicated to public cryptology", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 561–613, IEEE Press, 1992.

[528] C.G. GÜNTHER, "Alternating step generators controlled by de Bruijn sequences", *Advances in Cryptology–EUROCRYPT '87 (LNCS 304)*, 5–14, 1988.

[529] ———, "A universal algorithm for homophonic coding", *Advances in Cryptology–*

EUROCRYPT '88 (LNCS 330), 405–414, 1988.

[530] ———, "An identity-based key-exchange protocol", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 29–37, 1990.

[531] H. GUSTAFSON, *Statistical Analysis of Symmetric Ciphers*, PhD thesis, Queensland University of Technology, 1996.

[532] H. GUSTAFSON, E. DAWSON, AND J. GOLIĆ, "Randomness measures related to subset occurrence", E. Dawson and J. Golić, editors, *Cryptography: Policy and Algorithms, International Conference, Brisbane, Queensland, Australia, July 1995 (LNCS 1029)*, 132–143, 1996.

[533] H. GUSTAFSON, E. DAWSON, L. NIELSEN, AND W. CAELLI, "A computer package for measuring the strength of encryption algorithms", *Computers & Security*, 13 (1994), 687–697.

[534] A. GUYOT, "OCAPI: Architecture of a VLSI coprocessor for the gcd and extended gcd of large numbers", *Proceedings of the 10th IEEE Symposium on Computer Arithmetic*, 226–231, IEEE Press, 1991.

[535] S. HABER AND W.S. STORNETTA, "How to time-stamp a digital document", *Journal of Cryptology*, 3 (1991), 99–111.

[536] J.L. HAFNER AND K.S. MCCURLEY, "On the distribution of running times of certain integer factoring algorithms", *Journal of Algorithms*, 10 (1989), 531–556.

[537] ———, "A rigorous subexponential algorithm for computation of class groups", *Journal of the American Mathematical Society*, 2 (1989), 837–850.

[538] T. HANSEN AND G.L. MULLEN, "Primitive polynomials over finite fields", *Mathematics of Computation*, 59 (1992), 639–643.

[539] G.H. HARDY, *A Mathematician's Apology*, Cambridge University Press, London, 1967.

[540] G.H. HARDY AND E.M. WRIGHT, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 5th edition, 1979.

[541] C. HARPES, G.G. KRAMER, AND J.L. MASSEY, "A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 24–38, 1995.

[542] V. HARRIS, "An algorithm for finding the greatest common divisor", *Fibonacci Quarterly*, 8 (1970), 102–103.

[543] J. HÅSTAD, A.W. SCHRIFT, AND A. SHAMIR, "The discrete logarithm modulo a composite hides $O(n)$ bits", *Journal of Computer and System Sciences*, 47 (1993), 376–404.

[544] J. HÅSTAD, "Solving simultaneous modular equations of low degree", *SIAM Journal on Computing*, 17 (1988), 336–341.

[545] ———, "Pseudo-random generators under uniform assumptions", *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, 395–404, 1990.

[546] R. HEIMAN, "A note on discrete logarithms with special structure", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 454–457, 1993.

[547] ———, "Secure audio teleconferencing: A practical solution", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 437–448, 1993.

[548] M.E. HELLMAN, "An extension of the Shannon theory approach to cryptography", *IEEE Transactions on Information Theory*, 23 (1977), 289–294.

[549] ———, "A cryptanalytic time-memory tradeoff", *IEEE Transactions on Information Theory*, 26 (1980), 401–406.

[550] M.E. HELLMAN AND C.E. BACH, "Method and apparatus for use in public-key data encryption system", U.S. Patent # 4,633,036, 30 Dec 1986.

[551] M.E. HELLMAN, B.W. DIFFIE, AND R.C. MERKLE, "Cryptographic apparatus and method", U.S. Patent # 4,200,770, 29 Apr 1980.

[552] M.E. HELLMAN, R. MERKLE, R. SCHROEPPEL, L. WASHINGTON, W. DIFFIE, S. POHLIG, AND P. SCHWEITZER, "Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard", Technical Report SEL 76-042, Information Systems Laboratory, Stanford University, Palo Alto, California, Sept. 9 1976 (revised Nov 10 1976).

[553] M.E. HELLMAN AND R.C. MERKLE, "Public key cryptographic apparatus and method", U.S. Patent # 4,218,582, 19 Aug 1980.

[554] M.E. HELLMAN AND S.C. POHLIG, "Exponentiation cryptographic apparatus and method", U.S. Patent # 4,424,414, 3 Jan 1984.

[555] M.E. HELLMAN AND J.M. REYNERI, "Fast computation of discrete logarithms in $\mathrm{GF}(q)$", *Advances in Cryptology–Proceedings of Crypto 82*, 3–13, 1983.

[556] I.N. HERSTEIN, *Topics in Algebra*, Xerox College Pub., Lexington, Massachusetts, 2nd edition, 1975.

[557] L.S. HILL, "Cryptography in an algebraic alphabet", *American Mathematical Monthly*, 36 (1929), 306–312.

[558] L.J. HOFFMAN, *Modern Methods for Computer Security and Privacy*, Prentice Hall, Englewood Cliffs, New Jersey, 1977.

[559] R.V. HOGG AND E.A. TANIS, *Probability and statistical inference*, Macmillan Publishing Company, New York, 3rd edition, 1988.

[560] W. HOHL, X. LAI, T. MEIER, AND C. WALDVOGEL, "Security of iterated hash functions based on block ciphers", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 379–390, 1994.

[561] S.-M. HONG, S.-Y. OH, AND H. YOON, "New modular multiplication algorithms for fast modular exponentiation", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 166–177, 1996.

[562] P. HORSTER AND H.-J. KNOBLOCH, "Discrete logarithm based protocols", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 399–408, 1991.

[563] P. HORSTER, M. MICHELS, AND H. PETERSEN, "Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 224–237, 1995.

[564] P. HORSTER AND H. PETERSEN, "Generalized ElGamal signatures (in German)", *Sicherheit in Informationssystemen, Proceedings der Fachtagung SIS'94*, 89–106, Verlag der Fachvereine Zürich, 1994.

[565] T.W. HUNGERFORD, *Algebra*, Holt, Rinehart and Winston, New York, 1974.

[566] K. HWANG, *Computer Arithmetic, Principles, Architecture and Design*, John Wiley & Sons, New York, 1979.

[567] C. I'ANSON AND C. MITCHELL, "Security defects in CCITT Recommendation X.509 – The directory authentication framework", *Computer Communication Review*, 20 (1990), 30–34.

[568] R. IMPAGLIAZZO, L. LEVIN, AND M. LUBY, "Pseudo-random generation from one-way functions", *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, 12–24, 1989.

[569] R. IMPAGLIAZZO AND M. NAOR, "Efficient cryptographic schemes provably as secure as subset sum", *Proceedings of the IEEE 30th Annual Symposium on Foundations of Computer Science*, 236–241, 1989.

[570] I. INGEMARSSON AND G.J. SIMMONS, "A protocol to set up shared secret schemes without the assistance of a mutually trusted party", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 266–282, 1991.

[571] I. INGEMARSSON, D.T. TANG, AND C.K. WONG, "A conference key distribution system", *IEEE Transactions on Information Theory*, 28 (1982), 714–720.

[572] K. IRELAND AND M. ROSEN, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 2nd edition, 1990.

[573] ISO 7498-2, "Information processing systems – Open Systems Interconnection – Basic reference model – Part 2: Security architecture", International Organization for Standardization, Geneva, Switzerland, 1989 (first edition) (equivalent to ITU-T Rec. X.800).

[574] ISO 8372, "Information processing – Modes of operation for a 64-bit block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1987 (first edition; confirmed 1992).

[575] ISO 8730, "Banking – Requirements for message authentication (wholesale)", International Organization for Standardization, Geneva, Switzerland, 1990 (second edition).

[576] ISO 8731-1, "Banking – Approved algorithms for message authentication – Part 1: DEA", International Organization for Standardization, Geneva, Switzerland, 1987 (first edition; confirmed 1992).

[577] ISO 8731-2, "Banking – Approved algorithms for message authentication – Part 2: Message authenticator algorithm", International Organization for Standardization, Geneva, Switzerland, 1992 (second edition).

[578] ISO 8732, "Banking – Key management (wholesale)", International Organization for Standardization, Geneva, Switzerland, 1988 (first edition).

[579] ISO 9564-1, "Banking – Personal Identification Number management and security – Part 1: PIN protection principles and techniques", International Organization for Standardization, Geneva, Switzerland, 1990.

[580] ISO 9564-2, "Banking – Personal Identification Number management and security – Part 2: Approved algorithm(s) for PIN encipherment", International Organization for Standardization, Geneva, Switzerland, 1991.

[581] ISO 9807, "Banking and related financial services – Requirements for message authentication (retail)", International Organization for Standardization, Geneva, Switzerland, 1991.

[582] ISO 10126-1, "Banking – Procedures for message encipherment (wholesale) – Part 1: General principles", International Organization for Standardization, Geneva, Switzerland, 1991.

[583] ISO 10126-2, "Banking – Procedures for message encipherment (wholesale) – Part 2: Algorithms", International Organization for Standardization, Geneva, Switzerland, 1991.

[584] ISO 10202-7, "Financial transaction cards – Security architecture of financial transaction systems using integrated circuit cards – Part 7: Key management", draft (DIS), 1994.

[585] ISO 11131, "Banking – Financial institution sign-on authentication", International Organization for Standardization, Geneva, Switzerland, 1992.

[586] ISO 11166-1, "Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats", International Organization for Standardization, Geneva, Switzerland, 1994.

[587] ISO 11166-2, "Banking – Key management by means of asymmetric algorithms – Part 2: Approved algorithms using the RSA cryptosystem", International Organization for Standardization, Geneva, Switzerland, 1995.

[588] ISO 11568-1, "Banking – Key management (retail) – Part 1: Introduction to key management", International Organization for Standardization, Geneva, Switzerland, 1994.

[589] ISO 11568-2, "Banking – Key management (retail) – Part 2: Key management techniques for symmetric ciphers", International Organization for Standardization, Geneva, Switzerland, 1994.

[590] ISO 11568-3, "Banking – Key management (retail) – Part 3: Key life cycle for symmetric ciphers", International Organization for Standardization, Geneva, Switzerland, 1994.

[591] ISO 11568-4, "Banking – Key management (retail) – Part 4: Key management techniques using public key cryptography", draft (DIS), 1996.

[592] ISO 11568-5, "Banking – Key management (retail) – Part 5: Key life cycle for public key cryptosystems", draft (DIS), 1996.

[593] ISO 11568-6, "Banking – Key management (retail) – Part 6: Key management schemes", draft (CD), 1996.

[594] ISO/IEC 9594-1, "Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models, and services", International Organization for Standardization, Geneva, Switzerland, 1995 (equivalent to ITU-T Rec. X.500, 1993).

[595] ISO/IEC 9594-8, "Information technology – Open Systems Interconnection – The Directory: Authentication framework", International Organization for Standardization, Geneva, Switzerland, 1995 (equivalent to ITU-T Rec. X.509, 1993).

[596] ISO/IEC 9796, "Information technology – Security techniques – Digital signature scheme giving message recovery", International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).

[597] ISO/IEC 9797, "Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1994 (second edition).

[598] ISO/IEC 9798-1, "Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model", International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).

[599] ISO/IEC 9798-2, "Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms", International Organization for Standardization, Geneva, Switzerland, 1994 (first edition).

[600] ISO/IEC 9798-3, "Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authen-

tication using a public-key algorithm", International Organization for Standardization, Geneva, Switzerland, 1993 (first edition).

[601] ISO/IEC 9798-4, "Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function", International Organization for Standardization, Geneva, Switzerland, 1995 (first edition).

[602] ISO/IEC 9798-5, "Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero knowledge techniques", draft (CD), 1996.

[603] ISO/IEC 9979, "Data cryptographic techniques – Procedures for the registration of cryptographic algorithms", International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).

[604] ISO/IEC 10116, "Information processing – Modes of operation for an n-bit block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).

[605] ISO/IEC 10118-1, "Information technology – Security techniques – Hash-functions – Part 1: General", International Organization for Standardization, Geneva, Switzerland, 1994.

[606] ISO/IEC 10118-2, "Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm", International Organization for Standardization, Geneva, Switzerland, 1994.

[607] ISO/IEC 10118-3, "Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions", draft (CD), 1996.

[608] ISO/IEC 10118-4, "Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic", draft (CD), 1996.

[609] ISO/IEC 10181-1, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 1: Overview", International Organization for Standardization, Geneva, Switzerland, 1996 (equivalent to ITU-T Rec. X.810, 1995).

[610] ISO/IEC 10181-2, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 2: Authentication framework", International Organization for Standardization, Geneva, Switzerland, 1996 (equivalent to ITU-T Rec. X.811, 1995).

[611] ISO/IEC 10181-3, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 3: Access control framework", 1996.

[612] ISO/IEC 10181-4, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 4: Non-repudiation framework", 1996.

[613] ISO/IEC 10181-5, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 5: Confidentiality framework", 1996.

[614] ISO/IEC 10181-6, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 6: Integrity framework", 1996.

[615] ISO/IEC 10181-7, "Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 7: Security audit and alarms framework", 1996.

[616] ISO/IEC 11770-1, "Information technology – Security techniques – Key management – Part 1: Framework", draft (DIS), 1996.

[617] ISO/IEC 11770-2, "Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques", International Organization for Standardization, Geneva, Switzerland, 1996 (first edition).

[618] ISO/IEC 11770-3, "Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques", draft (DIS), 1996.

[619] ISO/IEC 13888-1, "Information technology – Security techniques – Non-repudiation – Part 1: General model", draft (CD), 1996.

[620] ISO/IEC 13888-2, "Information technology – Security techniques – Non-repudiation – Part 2: Using symmetric encipherment algorithms", draft (CD), 1996.

[621] ISO/IEC 13888-3, "Information technology – Security techniques – Non-repudiation – Part 3: Using asymmetric techniques", draft (CD), 1996.

[622] ISO/IEC 14888-1, "Information technology – Security techniques – Digital signatures with appendix – Part 1: General", draft (CD), 1996.

[623] ISO/IEC 14888-2, "Information technology – Security techniques – Digital signatures with appendix – Part 2: Identity-based mechanisms", draft (CD), 1996.

[624] ISO/IEC 14888-3, "Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms", draft (CD), 1996.

[625] M. ITO, A. SAITO, AND T. NISHIZEKI, "Secret sharing scheme realizing general access structure", *IEEE Global Telecommunications Conference*, 99–102, 1987.

[626] ITU-T REC. X.509 (REVISED), "The Directory – Authentication framework", International Telecommunication Union, Geneva, Switzerland, 1993 (equivalent to ISO/IEC 9594-8:1994).

[627] ITU-T REC. X.509 (1993) TECHNICAL CORRIGENDUM 1, "The Directory – Authentication framework", International Telecommunication Union, Geneva, Switzerland, July 1995 (equivalent to Technical Corrigendum 1 to ISO/IEC 9594-8:1994).

[628] ITU-T REC. X.509 (1993) AMENDMENT 1: CERTIFICATE EXTENSIONS, "The Directory – Authentication framework", International Telecommunication Union, Geneva, Switzerland, July 1995 draft for JCT1 letter ballot (equivalent to Ammendment 1 to ISO/IEC 9594-8:1994).

[629] W.-A. JACKSON, K.M. MARTIN, AND C.M. O'KEEFE, "Multisecret threshold schemes", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 126–135, 1994.

[630] G. JAESCHKE, "On strong pseudoprimes to several bases", *Mathematics of Computation*, 61 (1993), 915–926.

[631] C.J.A. JANSEN AND D.E. BOEKEE, "On the significance of the directed acyclic word graph in cryptology", *Advances in Cryptology–AUSCRYPT '90 (LNCS 453)*, 318–326, 1990.

[632] ———, "The shortest feedback shift register that can generate a given sequence", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 90–99, 1990.

[633] T. JEBELEAN, "Comparing several gcd algorithms", *Proceedings of the 11th Symposium on Computer Arithmetic*, 180–185, IEEE Press, 1993.

[634] J. JEDWAB AND C. MITCHELL, "Minimum weight modified signed-digit representations and fast exponentiation", *Electronics Letters*, 25 (August 17, 1989), 1171–1172.

[635] N. JEFFERIES, C. MITCHELL, AND M. WALKER, "A proposed architecture for trusted third party services", E. Dawson and J. Golić, editors, *Cryptography: Policy and Algorithms, International Conference, Brisbane, Queensland, Australia, July 1995 (LNCS 1029)*, 98–104, 1996.

[636] H.N. JENDAL, Y.J.B. KUHN, AND J.L. MASSEY, "An information-theoretic treatment of homophonic substitution", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 382–394, 1990.

[637] S.M. JENNINGS, "Multiplexed sequences: Some properties of the minimum polynomial", *Cryptography–Proceedings of the Workshop on Cryptography, Burg Feuerstein (LNCS 149)*, 189–206, 1983.

[638] T. JOHANSSON, G. KABATIANSKII, AND B. SMEETS, "On the relation between A-codes and codes correcting independent errors", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 1–11, 1994.

[639] D.B. JOHNSON, A. LE, W. MARTIN, S. MATYAS, AND J. WILKINS, "Hybrid key distribution scheme giving key record recovery", *IBM Technical Disclosure Bulletin*, 37 (1994), 5–16.

[640] D.B. JOHNSON AND S.M. MATYAS, "Asymmetric encryption: Evolution and enhancements", *CryptoBytes*, 2 (Spring 1996), 1–6.

[641] D.S. JOHNSON, "The NP-completeness column: an ongoing guide", *Journal of Algorithms*, 9 (1988), 426–444.

[642] R.W. JONES, "Some techniques for handling encipherment keys", *ICL Technical Journal*, 3 (1982), 175–188.

[643] R.R. JUENEMAN, "Analysis of certain aspects of output feedback mode", *Advances in Cryptology–Proceedings of Crypto 82*, 99–127, 1983.

[644] ———, "A high speed manipulation detection code", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 327–346, 1987.

[645] R.R. JUENEMAN, S.M. MATYAS, AND C.H. MEYER, "Message authentication with manipulation detection codes", *Proceedings of the 1983 IEEE Symposium on Security and Privacy*, 33–54, 1984.

[646] D. JUNGNICKEL, *Finite Fields: Structure and Arithmetics*, Bibliographisches Institut – Wissenschaftsverlag, Mannheim, 1993.

[647] M. JUST, E. KRANAKIS, D. KRIZANC, AND P. VAN OORSCHOT, "On key distribution via true broadcasting", *2nd ACM Conference on Computer and Communications Security*, 81–88, ACM Press, 1994.

[648] D. KAHN, *The Codebreakers*, Macmillan Publishing Company, New York, 1967.

[649] B.S. KALISKI JR., "A chosen message attack on Demytko's elliptic curve cryptosystem", *Journal of Cryptology*, to appear.

[650] ———, "A pseudo-random bit generator based on elliptic logarithms", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 84–103, 1987.

[651] ———, *Elliptic curves and cryptography: a pseudorandom bit generator and other tools*, PhD thesis, MIT Department of Electrical Engineering and Computer Science, 1988.

[652] ———, "Anderson's RSA trapdoor can be broken", *Electronics Letters*, 29 (July 22, 1993), 1387–1388.

[653] ———, "The Montgomery inverse and its applications", *IEEE Transactions on Computers*, 44 (1995), 1064–1065.

[654] B.S. KALISKI JR., R.L. RIVEST, AND A.T. SHERMAN, "Is the Data Encryption Standard a group? (Results of cycling experiments on DES)", *Journal of Cryptology*, 1 (1988), 3–36.

[655] B.S. KALISKI JR. AND M. ROBSHAW, "The secure use of RSA", *CryptoBytes*, 1 (Autumn 1995), 7–13.

[656] B.S. KALISKI JR. AND Y.L. YIN, "On differential and linear cryptanalysis of the RC5 encryption algorithm", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 171–184, 1995.

[657] E. KALTOFEN, "Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems", *Mathematics of Computation*, 64 (1995), 777–806.

[658] E. KALTOFEN AND V. SHOUP, "Subquadratic-time factoring of polynomials over finite fields", *Proceedings of the 27th Annual ACM Symposium on Theory of Computing*, 398–406, 1995.

[659] J. KAM AND G. DAVIDA, "Structured design of substitution-permutation encryption networks", *IEEE Transactions on Computers*, 28 (1979), 747–753.

[660] N. KAPIDZIC AND A. DAVIDSON, "A certificate management system: structure, functions and protocols", *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, 153–160, IEEE Computer Society Press, 1995.

[661] A. KARATSUBA AND YU. OFMAN, "Multiplication of multidigit numbers on automata", *Soviet Physics – Doklady*, 7 (1963), 595–596.

[662] E.D. KARNIN, J.W. GREENE, AND M.E. HELLMAN, "On secret sharing systems", *IEEE Transactions on Information Theory*, 29 (1983), 35–41.

[663] A. KEHNE, J. SCHÖWÄLDER, AND H. LANGENDÖRFER, "A nonce-based protocol for multiple authentications", *Operating Systems Review*, 26 (1992), 84–89.

[664] R. KEMMERER, C. MEADOWS, AND J. MILLEN, "Three systems for cryptographic protocol analysis", *Journal of Cryptology*, 7 (1994), 79–130.

[665] S. KENT, "Encryption-based protection protocols for interactive user-computer communication", MIT/LCS/TR-162 (M.Sc. thesis), MIT Laboratory for Computer Science, 1976.

[666] ———, "Internet privacy enhanced mail", *Communications of the ACM*, 36 (1993), 48–60.

[667] ———, "Internet security standards: past, present and future", *StandardView*, 2 (1994), 78–85.

[668] A. KERCKHOFFS, "La cryptographie militaire", *Journal des Sciences Militaires*, 9th Series (February 1883), 161–191.

[669] I. KESSLER AND H. KRAWCZYK, "Minimum buffer length and clock rate for the shrinking generator cryptosystem", IBM Research Report RC 19938, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., 1995.

[670] E. KEY, "An analysis of the structure and complexity of nonlinear binary sequence generators", *IEEE Transactions on Information Theory*, 22 (1976), 732–736.

[671] J. KILIAN AND T. LEIGHTON, "Fair cryptosystems, revisited: A rigorous approach to key-escrow", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 208–221, 1995.

[672] J. KILIAN AND P. ROGAWAY, "How to protect DES against exhaustive key search", *Advances in Cryptology–CRYPTO '96 (LNCS 1109)*, 252–267, 1996.

[673] S.-H. KIM AND C. POMERANCE, "The probability that a random probable prime is composite", *Mathematics of Computation*, 53 (1989), 721–741.

[674] M. KIMBERLEY, "Comparison of two statistical tests for keystream sequences", *Electronics Letters*, 23 (April 9, 1987), 365–366.

[675] A. KLAPPER, "The vulnerability of geometric sequences based on fields of odd characteristic", *Journal of Cryptology*, 7 (1994), 33–51.

[676] A. KLAPPER AND M. GORESKY, "Feedback shift registers, combiners with memory, and 2-adic span", *Journal of Cryptology*, to appear.

[677] ———, "2-Adic shift registers", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 174–178, Springer-Verlag, 1994.

[678] ———, "Cryptanalysis based on 2-adic rational approximation", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 262–273, 1995.

[679] ———, "Large period nearly de Bruijn FCSR sequences", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 263–273, 1995.

[680] D.V. KLEIN, "Foiling the cracker: a survey of, and improvements to, password security", *Proceedings of the 2nd USENIX UNIX Security Workshop*, 5–14, 1990.

[681] H.-J. KNOBLOCH, "A smart card implementation of the Fiat-Shamir identification scheme", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 87–95, 1988.

[682] L.R. KNUDSEN, "Cryptanalysis of LOKI", *Advances in Cryptology–ASIACRYPT '91 (LNCS 739)*, 22–35, 1993.

[683] ———, "Cryptanalysis of LOKI91", *Advances in Cryptology–AUSCRYPT '92 (LNCS 718)*, 196–208, 1993.

[684] ———, *Block Ciphers – Analysis, Design and Applications*, PhD thesis, Computer Science Department, Aarhus University (Denmark), 1994.

[685] ———, "A key-schedule weakness in SAFER K-64", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 274–286, 1995.

[686] ———, "Truncated and higher order differentials", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 196–211, Springer-Verlag, 1995.

[687] L.R. KNUDSEN AND T. BERSON, "Truncated differentials of SAFER", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 15–26, Springer-Verlag, 1996.

[688] L.R. KNUDSEN AND X. LAI, "New attacks on all double block length hash functions of hash rate 1, including the parallel-DM", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 410–418, 1995.

[689] L.R. KNUDSEN AND W. MEIER, "Improved differential attacks on RC5", *Advances in Cryptology–CRYPTO '96 (LNCS 1109)*, 216–228, 1996.

[690] L.R. KNUDSEN AND T. PEDERSEN, "On the difficulty of software key escrow", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 237–244, 1996.

[691] D.E. KNUTH, *The Art of Computer Programming – Fundamental Algorithms*, volume 1, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1973.

[692] ———, *The Art of Computer Programming – Seminumerical Algorithms*, volume 2, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1981.

[693] ———, *The Art of Computer Programming – Sorting and Searching*, volume 3, Addison-Wesley, Reading, Massachusetts, 1973.

[694] D.E. KNUTH AND L. TRABB PARDO, "Analysis of a simple factorization algorithm", *Theoretical Computer Science*, 3 (1976), 321–348.

[695] N. KOBLITZ, "Elliptic curve cryptosystems", *Mathematics of Computation*, 48 (1987), 203–209.

[696] ———, "Hyperelliptic cryptosystems", *Journal of Cryptology*, 1 (1989), 139–150.

[697] ———, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 2nd edition, 1994.

[698] C. KOÇ, "High-speed RSA implementation", Technical Report, RSA Laboratories, 1994.

[699] ———, "RSA hardware implementation", Technical Report TR-801, RSA Laboratories, 1996.

[700] C. KOÇ, T. ACAR, AND B.S. KALISKI JR., "Analyzing and comparing Montgomery multiplication algorithms", *IEEE Micro*, 16 (1996), 26–33.

[701] J.T. KOHL, "The use of encryption in Kerberos for network authentication", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 35–43, 1990.

[702] L.M. KOHNFELDER, "A method for certification", MIT Laboratory for Computer Science, unpublished (essentially pp.39-43 of [703]), 1978.

[703] ———, *Toward a practical public-key cryptosystem*, B.Sc. thesis, MIT Department of Electrical Engineering, 1978.

[704] A. KOLMOGOROV, "Three approaches to the definition of the concept 'quantity of information'", *Problemy Peredachi Informatsii*, 1 (1965), 3–11.

[705] A.G. KONHEIM, *Cryptography, A Primer*, John Wiley & Sons, New York, 1981.

[706] I. KOREN, *Computer Arithmetic Algorithms*, Prentice Hall, Englewood Cliffs, New Jersey, 1993.

[707] V.I. KORZHIK AND A.I. TURKIN, "Cryptanalysis of McEliece's public-key cryptosystem", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 68–70, 1991.

[708] K. KOYAMA, U. MAURER, T. OKAMOTO, AND S.A. VANSTONE, "New public-key schemes based on elliptic curves over the ring Z_n", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 252–266, 1992.

[709] K. KOYAMA AND R. TERADA, "How to strengthen DES-like cryptosystems against differential cryptanalysis", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, E76-A (1993), 63–69.

[710] E. KRANAKIS, *Primality and Cryptography*, John Wiley & Sons, Stuttgart, 1986.

[711] D.W. KRAVITZ, "Digital signature algorithm", U.S. Patent # 5,231,668, 27 Jul 1993.

[712] H. KRAWCZYK, "How to predict congruential generators", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 138–153, 1990.

[713] ———, "How to predict congruential generators", *Journal of Algorithms*, 13 (1992), 527–545. An earlier version appeared in [712].

[714] ———, "LFSR-based hashing and authentication", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 129–139, 1994.

[715] ———, "Secret sharing made short", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 136–146, 1994.

[716] ———, "The shrinking generator: Some practical considerations", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 45–46, Springer-Verlag, 1994.

[717] ———, "New hash functions for message authentication", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 301–310, 1995.

[718] ———, "SKEME: A versatile secure key exchange mechanism for Internet", *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, 114–127, IEEE Computer Society Press, 1996.

[719] Y. KURITA AND M. MATSUMOTO, "Primitive t-nomials ($t = 3{,}5$) over GF(2) whose degree is a Mersenne exponent ≤ 44497", *Mathematics of Computation*, 56 (1991), 817–821.

[720] K. KUROSAWA, T. ITO, AND M. TAKEUCHI, "Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number", *Cryptologia*, 12 (1988), 225–233.

[721] K. KUROSAWA, K. OKADA, AND S. TSUJII, "Low exponent attack against elliptic curve RSA", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 376–383, 1995.

[722] K. KUSUDA AND T. MATSUMOTO, "Optimization of time-memory trade-off cryptanalysis and its application to DES, FEAL-32, and Skipjack", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, E79-A (1996), 35–48.

[723] J.C. LAGARIAS, "Knapsack public key cryptosystems and diophantine approximation", *Advances in Cryptology–Proceedings of Crypto 83*, 3–23, 1984.

[724] ———, "Pseudorandom number generators in cryptography and number theory", C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, 115–143, American Mathematical Society, 1990.

[725] X. LAI, "Condition for the nonsingularity of a feedback shift-register over a general finite field", *IEEE Transactions on Information Theory*, 33 (1987), 747–749.

[726] ———, "On the design and security of block ciphers", ETH Series in Information Processing, J.L. Massey (editor), vol. 1, Hartung-Gorre Verlag Konstanz, Technische Hochschule (Zurich), 1992.

[727] X. LAI AND L.R. KNUDSEN, "Attacks on double block length hash functions", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 157–165, Springer-Verlag, 1994.

[728] X. LAI AND J.L. MASSEY, "A proposal for a new block encryption standard", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 389–404, 1991.

[729] ———, "Hash functions based on block ciphers", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 55–70, 1993.

[730] X. LAI, J.L. MASSEY, AND S. MURPHY, "Markov ciphers and differential cryptanalysis", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 17–38, 1991.

[731] X. LAI, R.A. RUEPPEL, AND J. WOOLLVEN, "A fast cryptographic checksum algorithm based on stream ciphers", *Advances in Cryptology–AUSCRYPT '92 (LNCS 718)*, 339–348, 1993.

[732] C.-S. LAIH, L. HARN, J.-Y. LEE, AND T. HWANG, "Dynamic threshold scheme based on the definition of cross-product in an n-dimensional linear space", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 286–298, 1990.

[733] C.-S. LAIH, F.-K. TU, AND W.-C TAI, "On the security of the Lucas function", *Information Processing Letters*, 53 (1995), 243–247.

[734] K.-Y. LAM AND T. BETH, "Timely authentication in distributed systems", Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, editors, *Second European Symposium on Research in Computer Security – ESORICS'92 (LNCS 648)*, 293–303, Springer-Verlag, 1992.

[735] K.-Y. LAM AND L.C.K. HUI, "Efficiency of $SS(I)$ square-and-multiply exponentiation algorithms", *Electronics Letters*, 30 (December 8, 1994), 2115–2116.

[736] B.A. LAMACCHIA AND A.M. ODLYZKO, "Computation of discrete logarithms in prime fields", *Designs, Codes and Cryptography*, 1 (1991), 47–62.

[737] ———, "Solving large sparse linear systems over finite fields", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 109–133, 1991.

[738] L. LAMPORT, "Constructing digital signatures from a one-way function", Technical report CSL-98, SRI International, Palo Alto, 1979.

[739] ———, "Password authentication with insecure communication", *Communications of the ACM*, 24 (1981), 770–772.

[740] B. LAMPSON, M. ABADI, M. BURROWS, AND E. WOBBER, "Authentication in distributed systems: Theory and practice", *ACM Transactions on Computer Systems*, 10 (1992), 265–310.

[741] S.K. LANGFORD AND M.E. HELLMAN, "Differential-linear cryptanalysis", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 17–25, 1994.

[742] P.J. LEE AND E.F. BRICKELL, "An observation on the security of McEliece's public-key cryptosystem", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 275–280, 1988.

[743] D.H. LEHMER, "Euclid's algorithm for large numbers", *American Mathematical Monthly*, 45 (1938), 227–233.

[744] D.H. LEHMER AND R.E. POWERS, "On factoring large numbers", *Bulletin of the AMS*, 37 (1931), 770–776.

[745] T. LEIGHTON AND S. MICALI, "Secret-key agreement without public-key cryptography", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 456–479, 1994.

[746] A.K. LENSTRA, "Posting to sci.crypt", April 11 1996.

[747] ———, "Primality testing", C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, 13–25, American Mathematical Society, 1990.

[748] A.K. LENSTRA AND H.W. LENSTRA JR., "Algorithms in number theory", J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, 674–715, Elsevier Science Publishers, 1990.

[749] ———, *The Development of the Number Field Sieve*, Springer-Verlag, Berlin, 1993.

[750] A.K. LENSTRA, H.W. LENSTRA JR., AND L. LOVÁSZ, "Factoring polynomials with rational coefficients", *Mathematische Annalen*, 261 (1982), 515–534.

[751] A.K. LENSTRA, H.W. LENSTRA JR., M.S. MANASSE, AND J.M. POLLARD, "The factorization of the ninth Fermat number", *Mathematics of Computation*, 61 (1993), 319–349.

[752] ———, "The number field sieve", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, 11–42, Springer-Verlag, 1993.

[753] A.K. LENSTRA AND M.S. MANASSE, "Factoring by electronic mail", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 355–371, 1990.

[754] ———, "Factoring with two large primes", *Mathematics of Computation*, 63 (1994), 785–798.

[755] A.K. LENSTRA, P. WINKLER, AND Y. YACOBI, "A key escrow system with warrant bounds", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 197–207, 1995.

[756] H.W. LENSTRA JR., "Factoring integers with elliptic curves", *Annals of Mathematics*, 126 (1987), 649–673.

[757] ———, "Finding isomorphisms between finite fields", *Mathematics of Computation*, 56 (1991), 329–347.

[758] ———, "On the Chor-Rivest knapsack cryptosystem", *Journal of Cryptology*, 3 (1991), 149–155.

[759] H.W. LENSTRA JR. AND C. POMERANCE, "A rigorous time bound for factoring integers", *Journal of the American Mathematical Society*, 5 (1992), 483–516.

[760] H.W. LENSTRA JR. AND R.J. SCHOOF, "Primitive normal bases for finite fields", *Mathematics of Computation*, 48 (1987), 217–231.

[761] L.A. LEVIN, "One-way functions and pseudorandom generators", *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, 363–365, 1985.

[762] J. LEVINE, *United States Cryptographic Patents 1861–1981*, Cryptologia, Inc., Terre Haute, Indiana, 1983.

[763] R. LIDL AND W.B. MÜLLER, "Permutation polynomials in RSA-cryptosystems", *Advances in Cryptology–Proceedings of Crypto 83*, 293–301, 1984.

[764] R. LIDL AND H. NIEDERREITER, *Finite Fields*, Cambridge University Press, Cambridge, 1984.

[765] A. LIEBL, "Authentication in distributed systems: A bibliography", *Operating Systems Review*, 27 (1993), 31–41.

[766] C.H. LIM AND P.J. LEE, "Another method for attaining security against adaptively chosen ciphertext attacks", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 420–434, 1994.

[767] ———, "More flexible exponentiation with precomputation", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 95–107, 1994.

[768] ———, "Server (prover/signer)-aided verification of identity proofs and signatures", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 64–78, 1995.

[769] S. LIN AND D. COSTELLO, *Error Control Coding: Fundamentals and Applications*, Prentice Hall, Englewood Cliffs, New Jersey, 1983.

[770] J. LIPSON, *Elements of Algebra and Algebraic Computing*, Addison-Wesley, Reading, Massachusetts, 1981.

[771] T.M.A. LOMAS, L. GONG, J.H. SALTZER, AND R.M. NEEDHAM, "Reducing risks from poorly chosen keys", *Operating Systems Review*, 23 (Special issue), 14–18. (Presented at: 12th ACM Symposium on Operating Systems Principles, Litchfield Park, Arizona, Dec. 1989).

[772] D.L. LONG AND A. WIGDERSON, "The discrete logarithm hides O(log n) bits", *SIAM Journal on Computing*, 17 (1988), 363–372.

[773] R. LOVORN, *Rigorous, subexponential algorithms for discrete logarithms over finite fields*, PhD thesis, University of Georgia, 1992.

[774] M. LUBY, *Pseudorandomness and Cryptographic Applications*, Princeton University Press, Princeton, New Jersey, 1996.

[775] M. LUBY AND C. RACKOFF, "Pseudorandom permutation generators and cryptographic composition", *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, 356–363, 1986.

[776] ———, "How to construct pseudorandom permutations from pseudorandom functions", *SIAM Journal on Computing*, 17 (1988), 373–386. An earlier version appeared in [775].

[777] S. LUCKS, "Faster Luby-Rackoff ciphers", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 189–203, Springer-Verlag, 1996.

[778] F.J. MACWILLIAMS AND N.J.A. SLOANE, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977 (fifth printing: 1986).

[779] W. MADRYGA, "A high performance encryption algorithm", J. Finch and E. Dougall, editors, *Computer Security: A Global Challenge, Proceedings of the Second IFIP International Conference on Computer Security*, 557–570, North-Holland, 1984.

[780] D.P. MAHER, "Crypto backup and key escrow", *Communications of the ACM*, 39 (1996), 48–53.

[781] W. MAO AND C. BOYD, "On the use of encryption in cryptographic protocols", P.G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, 251–262, Institute of Mathematics & Its Applications (IMA), 1995.

[782] G. MARSAGLIA, "A current view of random number generation", L. Billard, editor, *Computer Science and Statistics: Proceedings of the Sixteenth Symposium on the Interface*, 3–10, North-Holland, 1985.

[783] P. MARTIN-LÖF, "The definition of random sequences", *Information and Control*, 9 (1966), 602–619.

[784] J.L. MASSEY, "Shift-register synthesis and BCH decoding", *IEEE Transactions on Information Theory*, 15 (1969), 122–127.

[785] ———, "An introduction to contemporary cryptology", *Proceedings of the IEEE*, 76 (1988), 533–549.

[786] ———, "Contemporary cryptology: An introduction", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 1–39, IEEE Press, 1992. An earlier version appeared in [785].

[787] ———, "SAFER K-64: A byte-oriented block-ciphering algorithm", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 1–17, Springer-Verlag, 1994.

[788] ———, "SAFER K-64: One year later", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 212–241, Springer-Verlag, 1995.

[789] J.L. MASSEY AND I. INGEMARSSON, "The Rip Van Winkle cipher – A simple and provably computationally secure cipher with a finite key", *IEEE International Symposium on Information Theory (Abstracts)*, p.146, 1985.

[790] J.L. MASSEY AND X. LAI, "Device for converting a digital block and the use thereof", European Patent # 482,154, 29 Apr 1992.

[791] ———, "Device for the conversion of a digital block and use of same", U.S. Patent # 5,214,703, 25 May 1993.

[792] J.L. MASSEY AND J.K. OMURA, "Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission", U.S. Patent # 4,567,600, 28 Jan 1986.

[793] J.L. MASSEY AND R.A. RUEPPEL, "Linear ciphers and random sequence generators with multiple clocks", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 74–87, 1985.

[794] J.L. MASSEY AND S. SERCONEK, "A Fourier transform approach to the linear complexity of nonlinearly filtered sequences", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 332–340, 1994.

[795] M. MATSUI, "The first experimental cryptanalysis of the Data Encryption Standard", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 1–11, 1994.

[796] ———, "Linear cryptanalysis method for DES cipher", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 386–397, 1994.

[797] ———, "On correlation between the order of S-boxes and the strength of DES", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 366–375, 1995.

[798] M. MATSUI AND A. YAMAGISHI, "A new method for known plaintext attack of FEAL cipher", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 81–91, 1993.

[799] T. MATSUMOTO AND H. IMAI, "On the key predistribution system: A practical solution to the key distribution problem", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 185–193, 1988.

[800] T. MATSUMOTO, Y. TAKASHIMA, AND H. IMAI, "On seeking smart public-key-distribution systems", *The Transactions of the IECE of Japan*, E69 (1986), 99–106.

[801] S.M. MATYAS, "Digital signatures – an overview", *Computer Networks*, 3 (1979), 87–94.

[802] ———, "Key handling with control vectors", *IBM Systems Journal*, 30 (1991), 151–174.

[803] ———, "Key processing with control vectors", *Journal of Cryptology*, 3 (1991), 113–136.

[804] S.M. MATYAS AND C.H. MEYER, "Generation, distribution, and installation of cryptographic keys", *IBM Systems Journal*, 17 (1978), 126–137.

[805] S.M. MATYAS, C.H. MEYER, AND J. OSEAS, "Generating strong one-way functions with cryptographic algorithm", *IBM Technical Disclosure Bulletin*, 27 (1985), 5658–5659.

[806] S.M. MATYAS, C.H.W. MEYER, AND B.O. BRACHTL, "Controlled use of cryptographic keys via generating station established control values", U.S. Patent # 4,850,017, 18 Jul 1989.

[807] U. MAURER, "Fast generation of secure RSA-moduli with almost maximal diversity", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 636–647, 1990.

[808] ———, "New approaches to the design of self-synchronizing stream ciphers", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 458–471, 1991.

[809] ———, "A provably-secure strongly-randomized cipher", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 361–373, 1991.

[810] ———, "A universal statistical test for random bit generators", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 409–420, 1991.

[811] ———, "Conditionally-perfect secrecy and a provably-secure randomized cipher", *Journal of Cryptology*, 5 (1992), 53–66. An earlier version appeared in [809].

[812] ———, "Some number-theoretic conjectures and their relation to the generation of cryptographic primes", C. Mitchell, editor, *Cryptography and Coding II*, volume 33 of *Institute of Mathematics & Its Applications (IMA)*, 173–191, Clarendon Press, 1992.

[813] ———, "A universal statistical test for random bit generators", *Journal of Cryptology*, 5 (1992), 89–105. An earlier version appeared in [810].

[814] ———, "Factoring with an oracle", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 429–436, 1993.

[815] ———, "Secret key agreement by public discussion from common information", *IEEE Transactions on Information Theory*, 39 (1993), 733–742.

[816] ———, "A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 239–255, 1993.

[817] ———, "Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 271–281, 1994.

[818] ———, "Fast generation of prime numbers and secure public-key cryptographic parameters", *Journal of Cryptology*, 8 (1995), 123–155. An earlier version appeared in [807].

[819] ———, "The role of information theory in cryptography", P.G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, 49–71, Institute of Mathematics & Its Applications (IMA), 1995.

[820] U. MAURER AND J.L. MASSEY, "Perfect local randomness in pseudo-random sequences", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 100–112, 1990.

[821] ———, "Local randomness in pseudorandom sequences", *Journal of Cryptology*, 4 (1991), 135–149. An earlier version appeared in [820].

[822] ———, "Cascade ciphers: The importance of being first", *Journal of Cryptology*, 6 (1993), 55–61.

[823] U. MAURER AND Y. YACOBI, "Non-interactive public-key cryptography", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 498–507, 1991.

[824] ———, "A remark on a non-interactive public-key distribution system", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 458–460, 1993.

[825] K.S. MCCURLEY, "A key distribution system equivalent to factoring", *Journal of Cryptology*, 1 (1988), 95–105.

[826] ———, "Cryptographic key distribution and computation in class groups", R.A. Mollin, editor, *Number Theory and Applications*, 459–479, Kluwer Academic Publishers, 1989.

[827] ———, "The discrete logarithm problem", C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, 49–74, American Mathematical Society, 1990.

[828] R.J. MCELIECE, "A public-key cryptosystem based on algebraic coding theory", DSN progress report #42-44, Jet Propulsion Laboratory, Pasadena, California, 1978.

[829] ———, *The Theory of Information and Coding: A Mathematical Framework for Communication*, Cambridge University Press, Cambridge, 1984.

[830] ———, *Finite Fields for Computer Scientists and Engineeers*, Kluwer Academic Publishers, Boston, 1987.

[831] C.A. MEADOWS, "Formal verification of cryptographic protocols: a survey", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 133–150, 1995.

[832] W. MEIER, "On the security of the IDEA block cipher", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 371–385, 1994.

[833] W. MEIER AND O. STAFFELBACH, "Fast correlation attacks on stream ciphers", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 301–314, 1988.

[834] ———, "Fast correlation attacks on certain stream ciphers", *Journal of Cryptology*, 1 (1989), 159–176. An earlier version appeared in [833].

[835] ———, "Analysis of pseudo random sequences generated by cellular automata", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 186–199, 1991.

[836] ———, "Correlation properties of combiners with memory in stream ciphers", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 204–213, 1991.

[837] ———, "Correlation properties of combiners with memory in stream ciphers", *Journal of Cryptology*, 5 (1992), 67–86. An earlier version appeared in [836].

[838] ———, "The self-shrinking generator", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 205–214, 1995.

[839] S. MENDES AND C. HUITEMA, "A new approach to the X.509 framework: allowing a global authentication infrastructure without a global trust model", *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, 172–189, IEEE Computer Society Press, 1995.

[840] A. MENEZES, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston, 1993.

[841] A. MENEZES, I. BLAKE, X. GAO, R. MULLIN, S. VANSTONE, AND T. YAGHOOBIAN, *Applications of Finite Fields*, Kluwer Academic Publishers, Boston, 1993.

[842] A. MENEZES, T. OKAMOTO, AND S. VANSTONE, "Reducing elliptic curve logarithms to logarithms in a finite field", *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, 80–89, 1991.

[843] ———, "Reducing elliptic curve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, 39 (1993), 1639–1646. An earlier version appeared in [842].

[844] A. MENEZES, M. QU, AND S. VANSTONE, "Some new key agreement protocols providing implicit authentication", workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC'95), Ottawa, Canada, May 18–19 1995.

[845] R. MENICOCCI, "Cryptanalysis of a two-stage Gollmann cascade generator", W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy*, 62–69, 1993.

[846] R.C. MERKLE, "Digital signature system and method based on a conventional encryption function", U.S. Patent # 4,881,264, 14 Nov 1989.

[847] ———, "Method and apparatus for data encryption", U.S. Patent # 5,003,597, 26 Mar 1991.

[848] ———, "Method of providing digital signatures", U.S. Patent # 4,309,569, 5 Jan 1982.

[849] ———, "Secure communications over insecure channels", *Communications of the ACM*, 21 (1978), 294–299.

[850] ———, *Secrecy, Authentication, and Public Key Systems*, UMI Research Press, Ann Arbor, Michigan, 1979.

[851] ———, "Secrecy, authentication, and public key systems", Technical Report No.1979-1, Information Systems Laboratory, Stanford University, Palo Alto, California, 1979. Also available as [850].

[852] ———, "Protocols for public key cryptosystems", *Proceedings of the 1980 IEEE Symposium on Security and Privacy*, 122–134, 1980.

[853] ———, "A certified digital signature", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 218–238, 1990.

[854] ———, "A fast software one-way hash function", *Journal of Cryptology*, 3 (1990), 43–58.

[855] ———, "One way hash functions and DES", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 428–446, 1990.

[856] ———, "Fast software encryption functions", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 476–501, 1991.

[857] R.C. MERKLE AND M.E. HELLMAN, "Hiding information and signatures in trapdoor knapsacks", *IEEE Transactions on Information Theory*, 24 (1978), 525–530.

[858] ———, "On the security of multiple encryption", *Communications of the ACM*, 24 (1981), 465–467.

[859] C.H. MEYER AND S.M. MATYAS, *Cryptography: A New Dimension in Computer Data Security*, John Wiley & Sons, New York, 1982 (third printing).

[860] C.H. MEYER AND M. SCHILLING, "Secure program load with manipulation detection code", *Proceedings of the 6th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'88)*, 111–130, 1988.

[861] S. MICALI, "Fair cryptosystems and methods of use", U.S. Patent # 5,276,737, 4 Jan 1994.

[862] ———, "Fair cryptosystems and methods of use", U.S. Patent # 5,315,658, 24 May 1994 (continuation-in-part of 5,276,737).

[863] ———, "Fair public-key cryptosystems", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 113–138, 1993.

[864] S. MICALI, O. GOLDREICH, AND S. EVEN, "On-line/off-line digital signing", U.S. Patent # 5,016,274, 14 May 1991.

[865] S. MICALI, C. RACKOFF, AND B. SLOAN, "The notion of security for probabilistic cryptosystems", *SIAM Journal on Computing*, 17 (1988), 412–426.

[866] S. MICALI AND C.P. SCHNORR, "Efficient, perfect random number generators", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 173–198, 1990.

[867] ———, "Efficient, perfect polynomial random number generators", *Journal of Cryptology*, 3 (1991), 157–172. An earlier version appeared in [866].

[868] S. MICALI AND A. SHAMIR, "An improvement of the Fiat-Shamir identification and signature scheme", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 244–247, 1990.

[869] S. MICALI AND R. SIDNEY, "A simple method for generating and sharing pseudo-random functions, with applications to Clipper-like key escrow systems", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 185–196, 1995.

[870] P. MIHAILESCU, "Fast generation of provable primes using search in arithmetic progressions", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 282–293, 1994.

[871] M.J. MIHALJEVIĆ, "A security examination of the self-shrinking generator", presentation at 5th IMA Conference on Cryptography and Coding, Cirencester, U.K., December 1995.

[872] ———, "An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure", *Advances in Cryptology–AUSCRYPT '92 (LNCS 718)*, 349–356, 1993.

[873] ———, "A correlation attack on the binary sequence generators with time-varying output function", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 67–79, 1995.

[874] M.J. MIHALJEVIĆ AND J.D. GOLIĆ, "A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence", *Advances in Cryptology–AUSCRYPT '90 (LNCS 453)*, 165–175, 1990.

[875] ———, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 124–137, 1993.

[876] G.L. MILLER, "Riemann's hypothesis and tests for primality", *Journal of Computer and System Sciences*, 13 (1976), 300–317.

[877] S.P. MILLER, B.C. NEUMAN, J.I. SCHILLER, AND J.H. SALTZER, "Kerberos authentication and authorization system", Section E.2.1 of Project Athena Technical Plan, MIT, Cambridge, Massachusetts, 1987.

[878] V.S. MILLER, "Use of elliptic curves in cryptography", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 417–426, 1986.

[879] C. MITCHELL, "A storage complexity based analogue of Maurer key establishment using public channels", C. Boyd, editor, *Cryptography and Coding, 5th IMA Conference, Proceedings*, 84–93, Institute of Mathematics & Its Applications (IMA), 1995.

[880] ———, "Limitations of challenge-response entity authentication", *Electronics Letters*, 25 (August 17, 1989), 1195–1196.

[881] C. MITCHELL AND F. PIPER, "Key storage in secure networks", *Discrete Applied Mathematics*, 21 (1988), 215–228.

[882] C. MITCHELL, F. PIPER, AND P. WILD, "Digital signatures", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 325–378, IEEE Press, 1992.

[883] A. MITROPOULOS AND H. MEIJER, "Zero knowledge proofs – a survey", Technical Report No. 90-IR-05, Queen's University at Kingston, Kingston, Ontario, Canada, 1990.

[884] S. MIYAGUCHI, "The FEAL cipher family", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 627–638, 1991.

[885] S. MIYAGUCHI, S. KURIHARA, K. OHTA, AND H. MORITA, "Expansion of FEAL cipher", *NTT Review*, 2 (1990), 117–127.

[886] S. MIYAGUCHI, K. OHTA, AND M. IWATA, "128-bit hash function (N-hash)", *NTT Review*, 2 (1990), 128–132.

[887] S. MIYAGUCHI, A. SHIRAISHI, AND A. SHIMIZU, "Fast data encipherment algorithm FEAL-8", *Review of the Electrical Communications Laboratories*, 36 (1988), 433–437.

[888] A. MIYAJI AND M. TATEBAYASHI, "Public key cryptosystem with an elliptic curve", U.S. Patent # 5,272,755, 21 Dec 1993.

[889] ———, "Method of privacy communication using elliptic curves", U.S. Patent # 5,351,297, 27 Sep 1994 (continuation-in-part of 5,272,755).

[890] S.B. MOHAN AND B.S. ADIGA, "Fast algorithms for implementing RSA public key cryptosystem", *Electronics Letters*, 21 (August 15, 1985), 761.

[891] R. MOLVA, G. TSUDIK, E. VAN HERREWEGHEN, AND S. ZATTI, "KryptoKnight authentication and key distribution system", Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, editors, *Second European Symposium on Research in Computer Security – ESORICS'92 (LNCS 648)*, 155–174, Springer-Verlag, 1992.

[892] L. MONIER, "Evaluation and comparison of two efficient probabilistic primality testing algorithms", *Theoretical Computer Science*, 12 (1980), 97–108.

[893] P. MONTGOMERY, "Modular multiplication without trial division", *Mathematics of Computation*, 44 (1985), 519–521.

[894] ———, "Speeding the Pollard and elliptic curve methods of factorization", *Mathematics of Computation*, 48 (1987), 243–264.

[895] P. MONTGOMERY AND R. SILVERMAN, "An FFT extension to the $P-1$ factoring algorithm", *Mathematics of Computation*, 54 (1990), 839–854.

[896] P.L. MONTGOMERY, "A block Lanczos algorithm for finding dependencies over $GF(2)$", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 106–120, 1995.

[897] A.M. MOOD, "The distribution theory of runs", *The Annals of Mathematical Statistics*, 11 (1940), 367–392.

[898] J.H. MOORE, "Protocol failures in cryptosystems", *Proceedings of the IEEE*, 76 (1988), 594–602.

[899] ———, "Protocol failures in cryptosystems", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 541–558, IEEE Press, 1992. Appeared earlier as [898].

[900] J.H. MOORE AND G.J. SIMMONS, "Cycle structure of the DES for keys having palindromic (or antipalindromic) sequences of round keys", *IEEE Transactions on Software Engineering*, 13 (1987), 262–273. An earlier version appeared in [901].

[901] ———, "Cycle structure of the DES with weak and semi-weak keys", *Advances in Cryptology–CRYPTO '86 (LNCS 263)*, 9–32, 1987.

[902] F. MORAIN, "Distributed primality proving and the primality of $(2^{3539} + 1)/3$", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 110–123, 1991.

[903] ———, "Prime values of partition numbers and the primality of $p_{1840926}$", LIX Research Report LIX/RR/92/11, Laboratoire d'Informatique de l'Ecole Polytechnique, France, June 1992.

[904] F. MORAIN AND J. OLIVOS, "Speeding up the computations on an elliptic curve using addition-subtraction chains", *Theoretical Informatics and Applications*, 24 (1990), 531–543.

[905] I.H. MORGAN AND G.L. MULLEN, "Primitive normal polynomials over finite fields", *Mathematics of Computation*, 63 (1994), 759–765.

[906] R. MORRIS, "The Hagelin cipher machine (M-209), Reconstruction of the internal settings", *Cryptologia*, 2 (1978), 267–278.

[907] R. MORRIS AND K. THOMPSON, "Password security: a case history", *Communications of the ACM*, 22 (1979), 594–597.

[908] M.A. MORRISON AND J. BRILLHART, "A method of factoring and the factorization of F_7", *Mathematics of Computation*, 29 (1975), 183–205.

[909] W.B. MÜLLER AND R. NÖBAUER, "Cryptanalysis of the Dickson-scheme", *Advances in Cryptology–EUROCRYPT '85 (LNCS 219)*, 50–61, 1986.

[910] W.B. MÜLLER AND W. NÖBAUER, "Some remarks on public-key cryptosystems", *Studia Scientiarum Mathematicarum Hungarica*, 16 (1981), 71–76.

[911] R. MULLIN, I. ONYSZCHUK, S. VANSTONE, AND R. WILSON, "Optimal normal bases in $GF(p^n)$", *Discrete Applied Mathematics*, 22 (1988/89), 149–161.

[912] S. MUND, "Ziv-Lempel complexity for periodic sequences and its cryptographic application", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 114–126, 1991.

[913] S. MURPHY, "The cryptanalysis of FEAL-4 with 20 chosen plaintexts", *Journal of Cryptology*, 2 (1990), 145–154.

[914] D. NACCACHE, "Can O.S.S. be repaired? – proposal for a new practical signature scheme", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 233–239, 1994.

[915] D. NACCACHE, D. M'RAÏHI, AND D. RAPHAELI, "Can Montgomery parasites be avoided? A design methodology based on key and cryptosystem modifications", *Designs, Codes and Cryptography*, 5 (1995), 73–80.

[916] D. NACCACHE, D. M'RAÏHI, S. VAUDENAY, AND D. RAPHAELI, "Can D.S.A. be improved? Complexity trade-offs with the digital signature standard", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 77–85, 1995.

[917] D. NACCACHE AND H. M'SILTI, "A new modulo computation algorithm", *Recherche Opérationnelle – Operations Research (RAIRO-OR)*, 24 (1990), 307–313.

[918] K. NAGASAKA, J.-S. SHIUE, AND C.-W. HO, "A fast algorithm of the Chinese remainder theorem and its application to Fibonacci number", G.E. Bergum, A.N. Philippou, and A.F. Horadam, editors, *Applications of Fibonacci Numbers, Proceedings of the Fourth International Conference on Fibonacci Numbers and their Applications*, 241–246, Kluwer Academic Publishers, 1991.

[919] M. NAOR AND A. SHAMIR, "Visual cryptography", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 1–12, 1995.

[920] M. NAOR AND M. YUNG, "Universal one-way hash functions and their cryptographic applications", *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, 33–43, 1989.

[921] ———, "Public-key cryptosystems provably secure against chosen ciphertext attacks", *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, 427–437, 1990.

[922] J. NECHVATAL, "Public key cryptography", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 177–288, IEEE Press, 1992.

[923] R.M. NEEDHAM AND M.D. SCHROEDER, "Using encryption for authentication in large networks of computers", *Communications of the ACM*, 21 (1978), 993–999.

[924] ———, "Authentication revisited", *Operating Systems Review*, 21 (1987), 7.

[925] B.C. NEUMAN AND S.G. STUBBLEBINE, "A note on the use of timestamps as nonces", *Operating Systems Review*, 27 (1993), 10–14.

[926] B.C. NEUMAN AND T. TS'O, "Kerberos: an authentication service for computer networks", *IEEE Communications Magazine*, 32 (September 1994), 33–38.

[927] H. NIEDERREITER, "The probabilistic theory of linear complexity", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 191–209, 1988.

[928] ———, "A combinatorial approach to probabilistic results on the linear-complexity profile of random sequences", *Journal of Cryptology*, 2 (1990), 105–112.

[929] ———, "Keystream sequences with a good linear complexity profile for every starting point", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 523–532, 1990.

[930] ———, "The linear complexity profile and the jump complexity of keystream sequences", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 174–188, 1991.

[931] K. NISHIMURA AND M. SIBUYA, "Probability to meet in the middle", *Journal of Cryptology*, 2 (1990), 13–22.

[932] I.M. NIVEN AND H.S. ZUCKERMAN, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 4th edition, 1980.

[933] M.J. NORRIS AND G.J. SIMMONS, "Algorithms for high-speed modular arithmetic", *Congressus Numerantium*, 31 (1981), 153–163.

[934] G. NORTON, "Extending the binary gcd algorithm", J. Calmet, editor, *Algebraic Algorithms and Error-Correcting Codes, 3rd International Conference, AAECC-3 (LNCS 229)*, 363–372, Springer-Verlag, 1986.

[935] K. NYBERG, "On one-pass authenticated key establishment schemes", workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC'95), Ottawa, Canada, May 18–19 1995.

[936] K. NYBERG AND R. RUEPPEL, "A new signature scheme based on the DSA giving message recovery", *1st ACM Conference on Computer and Communications Security*, 58–61, ACM Press, 1993.

[937] ———, "Weaknesses in some recent key agreement protocols", *Electronics Letters*, 30 (January 6, 1994), 26–27.

[938] ———, "Message recovery for signature schemes based on the discrete logarithm problem", *Designs, Codes and Cryptography*, 7 (1996), 61–81.

[939] A.M. ODLYZKO, "Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme", *IEEE Transactions on Information Theory*, 30 (1984), 594–601.

[940] ———, "Discrete logarithms in finite fields and their cryptographic significance", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 224–314, 1985.

[941] ———, "The rise and fall of knapsack cryptosystems", C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, 75–88, American Mathematical Society, 1990.

[942] ———, "Discrete logarithms and smooth polynomials", G.L. Mullen and P.J-S. Shiue, editors, *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemporary Mathematics*, 269–278, American Mathematical Society, 1994.

[943] K. OHTA AND K. AOKI, "Linear cryptanalysis of the Fast Data Encipherment Algorithm", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 12–16, 1994.

[944] K. OHTA AND T. OKAMOTO, "Practical extension of Fiat-Shamir scheme", *Electronics Letters*, 24 (July 21, 1988), 955–956.

[945] ———, "A modification of the Fiat-Shamir scheme", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 232–243, 1990.

[946] E. OKAMOTO AND K. TANAKA, "Key distribution system based on identification information", *IEEE Journal on Selected Areas in Communications*, 7 (1989), 481–485.

[947] T. OKAMOTO, "A single public-key authentication scheme for multiple users", *Systems and Computers in Japan*, 18 (1987), 14–24. Translated from *Denshi Tsushin Gakkai Ronbunshi* vol. 69-D no.10, October 1986, 1481–1489.

[948] ———, "A fast signature scheme based on congruential polynomial operations", *IEEE Transactions on Information Theory*, 36 (1990), 47–53.

[949] ———, "Provably secure and practical identification schemes and corresponding signature

schemes", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 31–53, 1993.

[950] ———, "Designated confirmer signatures and public-key encryption are equivalent", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 61–74, 1994.

[951] ———, "An efficient divisible electronic cash scheme", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 438–451, 1995.

[952] T. OKAMOTO, S. MIYAGUCHI, A. SHIRAISHI, AND T. KAWAOKA, "Signed document transmission system", U.S. Patent # 4,625,076, 25 Nov 1986.

[953] T. OKAMOTO AND A. SHIRAISHI, "A fast signature scheme based on quadratic inequalities", *Proceedings of the 1985 IEEE Symposium on Security and Privacy*, 123–132, 1985.

[954] T. OKAMOTO, A. SHIRAISHI, AND T. KAWAOKA, "Secure user authentication without password files", Technical Report NI83-92, I.E.C.E., Japan, January 1984. In Japanese.

[955] J. OLIVOS, "On vectorial addition chains", *Journal of Algorithms*, 2 (1981), 13–21.

[956] J.K. OMURA AND J.L. MASSEY, "Computational method and apparatus for finite field arithmetic", U.S. Patent # 4,587,627, 6 May 1986.

[957] H. ONG AND C.P. SCHNORR, "Fast signature generation with a Fiat Shamir-like scheme", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 432–440, 1991.

[958] H. ONG, C.P. SCHNORR, AND A. SHAMIR, "An efficient signature scheme based on quadratic equations", *Proceedings of the 16th Annual ACM Symposium on Theory of Computing*, 208–216, 1984.

[959] I.M. ONYSZCHUK, R.C. MULLIN, AND S.A. VANSTONE, "Computational method and apparatus for finite field multiplication", U.S. Patent # 4,745,568, 17 May 1988.

[960] G. ORTON, "A multiple-iterated trapdoor for dense compact knapsacks", *Advances in Cryptology–EUROCRYPT '94 (LNCS 950)*, 112–130, 1995.

[961] D. OTWAY AND O. REES, "Efficient and timely mutual authentication", *Operating Systems Review*, 21 (1987), 8–10.

[962] J.C. PAILLÈS AND M. GIRAULT, "CRIPT: A public-key based solution for secure data communications", *Proceedings of the 7th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'89)*, 171–185, 1989.

[963] C.H. PAPADIMITRIOU, *Computational Complexity*, Addison-Wesley, Reading, Massachusetts, 1994.

[964] S.-J. PARK, S.-J. LEE, AND S.-C. GOH, "On the security of the Gollmann cascades", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 148–156, 1995.

[965] J. PATARIN, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 33–48, 1996.

[966] J. PATARIN AND P. CHAUVAUD, "Improved algorithms for the permuted kernel problem", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 391–402, 1994.

[967] W. PENZHORN AND G. KÜHN, "Computation of low-weight parity checks for correlation attacks on stream ciphers", C. Boyd, editor, *Cryptography and Coding, 5th IMA Conference, Proceedings*, 74–83, Institute of Mathematics & Its Applications (IMA), 1995.

[968] R. PERALTA, "Simultaneous security of bits in the discrete log", *Advances in Cryptology–EUROCRYPT '85 (LNCS 219)*, 62–72, 1986.

[969] R. PERALTA AND V. SHOUP, "Primality testing with fewer random bits", *Computational Complexity*, 3 (1993), 355–367.

[970] A. PFITZMANN AND R. ASSMANN, "More efficient software implementations of (generalized) DES", *Computers & Security*, 12 (1993), 477–500.

[971] B. PFITZMANN AND M. WAIDNER, "Fail-stop signatures and their applications", *Proceedings of the 9th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'91)*, 145–160, 1991.

[972] ———, "Formal aspects of fail-stop signatures", Interner Bericht 22/90, Universität Karlsruhe, Germany, December 1990.

[973] S.J.D. PHOENIX AND P.D. TOWNSEND, "Quantum cryptography: protecting our future networks with quantum mechanics", C. Boyd, editor, *Cryptography and Coding, 5th IMA Conference, Proceedings*, 112–131, Institute of Mathematics & Its Applications (IMA), 1995.

[974] R. PINCH, "The Carmichael numbers up to 10^{15}", *Mathematics of Computation*, 61 (1993), 381–391.

[975] ——, "Some primality testing algorithms", *Notices of the American Mathematical Society*, 40 (1993), 1203–1210.

[976] ——, "Extending the Håstad attack to LUC", *Electronics Letters*, 31 (October 12, 1995), 1827–1828.

[977] ——, "Extending the Wiener attack to RSA-type cryptosystems", *Electronics Letters*, 31 (September 28, 1995), 1736–1738.

[978] V. PLESS, "Encryption schemes for computer confidentiality", *IEEE Transactions on Computers*, 26 (1977), 1133–1136.

[979] J.B. PLUMSTEAD, "Inferring a sequence generated by a linear congruence", *Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science*, 153–159, 1982.

[980] ——, "Inferring a sequence produced by a linear congruence", *Advances in Cryptology–Proceedings of Crypto 82*, 317–319, 1983.

[981] H.C. POCKLINGTON, "The determination of the prime or composite nature of large numbers by Fermat's theorem", *Proceedings of the Cambridge Philosophical Society*, 18 (1914), 29–30.

[982] S.C. POHLIG AND M.E. HELLMAN, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance", *IEEE Transactions on Information Theory*, 24 (1978), 106–110.

[983] D. POINTCHEVAL, "A new identification scheme based on the perceptrons problem", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 319–328, 1995.

[984] J.M. POLLARD, "Theorems on factorization and primality testing", *Proceedings of the Cambridge Philosophical Society*, 76 (1974), 521–528.

[985] ——, "A Monte Carlo method for factorization", *BIT*, 15 (1975), 331–334.

[986] ——, "Monte Carlo methods for index computation $\pmod p$", *Mathematics of Computation*, 32 (1978), 918–924.

[987] ——, "Factoring with cubic integers", A.K. Lenstra and H.W. Lenstra Jr., editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, 4–10, Springer-Verlag, 1993.

[988] J.M. POLLARD AND C. SCHNORR, "An efficient solution of the congruence $x^2 + ky^2 = m \pmod n$", *IEEE Transactions on Information Theory*, 33 (1987), 702–709.

[989] C. POMERANCE, "Analysis and comparison of some integer factoring algorithms", H.W. Lenstra Jr. and R. Tijdeman, editors, *Computational Methods in Number Theory, Part 1*, 89–139, Mathematisch Centrum, 1982.

[990] ——, "The quadratic sieve factoring algorithm", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 169–182, 1985.

[991] ——, "Fast, rigorous factorization and discrete logarithm algorithms", *Discrete Algorithms and Complexity*, 119–143, Academic Press, 1987.

[992] ——, "Very short primality proofs", *Mathematics of Computation*, 48 (1987), 315–322.

[993] ——, editor, *Cryptology and Computational Number Theory*, American Mathematical Society, Providence, Rhode Island, 1990.

[994] ——, "Factoring", C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, 27–47, American Mathematical Society, 1990.

[995] ——, "The number field sieve", W. Gautschi, editor, *Mathematics of Computation, 1943-1993: A Half-Century of Computation Mathematics*, volume 48 of *Proceedings of Symposia in Applied Mathematics*, 465–480, American Mathematical Society, 1994.

[996] C. POMERANCE, J.L. SELFRIDGE, AND S.S. WAGSTAFF JR., "The pseudoprimes to $25 \cdot 10^9$", *Mathematics of Computation*, 35 (1980), 1003–1026.

[997] C. POMERANCE AND J. SORENSON, "Counting the integers factorable via cyclotomic methods", *Journal of Algorithms*, 19 (1995), 250–265.

[998] G.J. POPEK AND C.S. KLINE, "Encryption and secure computer networks", *ACM Computing Surveys*, 11 (1979), 331–356.

[999] E. PRANGE, "An algorism for factoring $x^n - 1$ over a finite field", AFCRC-TN-59-775, Air Force Cambridge Research Center, 1959.

[1000] V.R. PRATT, "Every prime has a succinct certificate", *SIAM Journal on Computing*, 4 (1975), 214–220.

[1001] B. PRENEEL, "Standardization of cryptographic techniques", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 162–173, Springer-Verlag, 1993.

[1002] ———, "Cryptographic hash functions", *European Transactions on Telecommunications*, 5 (1994), 431–448.

[1003] ———, *Analysis and design of cryptographic hash functions*, PhD thesis, Katholieke Universiteit Leuven (Belgium), Jan. 1993.

[1004] ———, *Cryptographic Hash Functions*, Kluwer Academic Publishers, Boston, (to appear). Updated and expanded from [1003].

[1005] B. PRENEEL, R. GOVAERTS, AND J. VANDEWALLE, "Differential cryptanalysis of hash functions based on block ciphers", *1st ACM Conference on Computer and Communications Security*, 183–188, ACM Press, 1993.

[1006] ———, "Information authentication: Hash functions and digital signatures", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 87–131, Springer-Verlag, 1993.

[1007] ———, "Hash functions based on block ciphers: A synthetic approach", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 368–378, 1994.

[1008] B. PRENEEL, M. NUTTIN, V. RIJMEN, AND J. BUELENS, "Cryptanalysis of the CFB mode of the DES with a reduced number of rounds", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 212–223, 1994.

[1009] B. PRENEEL AND P. VAN OORSCHOT, "MDx-MAC and building fast MACs from hash functions", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 1–14, 1995.

[1010] ———, "On the security of two MAC algorithms", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 19–32, 1996.

[1011] N. PROCTOR, "A self-synchronizing cascaded cipher system with dynamic control of error propagation", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 174–190, 1985.

[1012] G.B. PURDY, "A high security log-in procedure", *Communications of the ACM*, 17 (1974), 442–445.

[1013] M. QU AND S.A. VANSTONE, "The knapsack problem in cryptography", *Contemporary Mathematics*, 168 (1994), 291–308.

[1014] K. QUINN, "Some constructions for key distribution patterns", *Designs, Codes and Cryptography*, 4 (1994), 177–191.

[1015] J.-J. QUISQUATER, "A digital signature scheme with extended recovery", preprint, 1995.

[1016] J.-J. QUISQUATER AND C. COUVREUR, "Fast decipherment algorithm for RSA public-key cryptosystem", *Electronics Letters*, 18 (October 14, 1982), 905–907.

[1017] J.-J. QUISQUATER AND J.-P. DELESCAILLE, "How easy is collision search? Application to DES", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 429–434, 1990.

[1018] ———, "How easy is collision search. New results and applications to DES", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 408–413, 1990.

[1019] J.-J. QUISQUATER AND M. GIRAULT, "$2n$-bit hash-functions using n-bit symmetric block cipher algorithms", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 102–109, 1990.

[1020] J.-J. QUISQUATER, L. GUILLOU, AND T. BERSON, "How to explain zero-knowledge protocols to your children", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 628–631, 1990.

[1021] M.O. RABIN, "Probabilistic algorithms", J.F. Traub, editor, *Algorithms and Complexity*, 21–40, Academic Press, 1976.

[1022] ———, "Digitalized signatures", R. DeMillo, D. Dobkin, A. Jones, and R. Lipton, editors, *Foundations of Secure Computation*, 155–168, Academic Press, 1978.

[1023] ———, "Digitalized signatures and public-key functions as intractable as factorization", MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[1024] ———, "Probabilistic algorithm for testing primality", *Journal of Number Theory*, 12 (1980), 128–138.

[1025] ———, "Probabilistic algorithms in finite fields", *SIAM Journal on Computing*, 9 (1980), 273–280.

[1026] ———, "Fingerprinting by random polynomials", TR-15-81, Center for Research in Computing Technology, Harvard University, 1981.

[1027] ———, "Efficient dispersal of information for security, load balancing, and fault tolerance", *Journal of the Association for Computing Machinery*, 36 (1989), 335–348.

[1028] T. RABIN AND M. BEN-OR, "Verifiable secret sharing and multiparty protocols with honest majority", *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, 73–85, 1989.

[1029] C. RACKOFF AND D.R. SIMON, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 433–444, 1992.

[1030] G. RAWLINS, *Compared to What? An Introduction to the Analysis of Algorithms*, Computer Science Press, New York, 1992.

[1031] G. REITWIESNER, "Binary arithmetic", *Advances in Computers*, 1 (1960), 231–308.

[1032] T. RENJI, "On finite automaton one-key cryptosystems", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 135–148, Springer-Verlag, 1994.

[1033] RFC 1319, "The MD2 message-digest algorithm", Internet Request for Comments 1319, B. Kaliski, April 1992 (updates RFC 1115, August 1989, J. Linn).

[1034] RFC 1320, "The MD4 message-digest algorithm", Internet Request for Comments 1320, R.L. Rivest, April 1992 (obsoletes RFC 1186, October 1990, R. Rivest).

[1035] RFC 1321, "The MD5 message-digest algorithm", Internet Request for Comments 1321, R.L. Rivest, April 1992 (presented at Rump Session of Crypto'91).

[1036] RFC 1421, "Privacy enhancement for Internet electronic mail – Part I: Message encryption and authentication procedures", Internet Request for Comments 1421, J. Linn, February 1993 (obsoletes RFC 1113 – September 1989; RFC 1040 – January 1988; and RFC 989 – February 1987, J. Linn).

[1037] RFC 1422, "Privacy enhancement for Internet electronic mail – Part II: Certificate-based key management", Internet Request for Comments 1422, S. Kent, February 1993 (obsoletes RFC 1114, August 1989, S. Kent and J. Linn).

[1038] RFC 1423, "Privacy enhancement for Internet electronic mail – Part III: Algorithms, modes, and identifiers", Internet Request for Comments 1423, D. Balenson, February 1993 (obsoletes RFC 1115, September 1989, J. Linn).

[1039] RFC 1424, "Privacy enhancement for Internet electronic mail – Part IV: Key certification and related services", Internet Request for Comments 1424, B. Kaliski, February 1993.

[1040] RFC 1508, "Generic security service application program interface", Internet Request for Comments 1508, J. Linn, September 1993.

[1041] RFC 1510, "The Kerberos network authentication service (V5)", Internet Request for Comments 1510, J. Kohl and C. Neuman, September 1993.

[1042] RFC 1521, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for specifying and describing the format of Internet message bodies", Internet Request for Comments 1521, N. Borenstein and N. Freed, September 1993 (obsoletes RFC 1341).

[1043] RFC 1750, "Randomness requirements for security", Internet Request for Comments 1750, D. Eastlake, S. Crocker and J. Schiller, December 1994.

[1044] RFC 1828, "IP authentication using keyed MD5", Internet Request for Comments 1828, P. Metzger and W. Simpson, August 1995.

[1045] RFC 1847, "Security multiparts for MIME: Multipart/signed and multipart/encrypted", Internet Request for Comments 1847, J. Galvin, S. Murphy, S. Crocker and N. Freed, October 1995.

[1046] RFC 1848, "MIME object security services", Internet Request for Comments 1848, S. Crocker, N. Freed, J. Galvin and S. Murphy, October 1995.

[1047] RFC 1938, "A one-time password system", Internet Request for Comments 1938, N. Haller and C. Metz, May 1996.

[1048] V. RIJMEN, J. DAEMEN, B. PRENEEL, A. BOSSELAERS, AND E. DE WIN, "The cipher SHARK", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 99–111, Springer-Verlag, 1996.

[1049] V. RIJMEN AND B. PRENEEL, "On weaknesses of non-surjective round functions", presented at the 2nd Workshop on Selected Areas in Cryptography (SAC'95), Ottawa, Canada, May 18–19 1995.

[1050] ———, "Improved characteristics for differential cryptanalysis of hash functions based on block ciphers", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 242–248, Springer-Verlag, 1995.

[1051] R.L. RIVEST, "Are 'strong' primes needed for RSA?", unpublished manuscript, 1991.

[1052] ———, "Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem", *Cryptologia*, 2 (1978), 62–65.

[1053] ———, "Statistical analysis of the Hagelin cryptograph", *Cryptologia*, 5 (1981), 27–32.

[1054] ———, "Cryptography", J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, 719–755, Elsevier Science Publishers, 1990.

[1055] ———, "The MD4 message digest algorithm", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 303–311, 1991.

[1056] ———, "The RC5 encryption algorithm", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 86–96, Springer-Verlag, 1995.

[1057] R.L. RIVEST AND A. SHAMIR, "How to expose an eavesdropper", *Communications of the ACM*, 27 (1984), 393–395.

[1058] ———, "Efficient factoring based on partial information", *Advances in Cryptology–EUROCRYPT '85 (LNCS 219)*, 31–34, 1986.

[1059] R.L. RIVEST, A. SHAMIR, AND L.M. ADLEMAN, "Cryptographic communications system and method", U.S. Patent # 4,405,829, 20 Sep 1983.

[1060] ———, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, 21 (1978), 120–126.

[1061] R.L. RIVEST AND A.T. SHERMAN, "Randomized encryption techniques", *Advances in Cryptology–Proceedings of Crypto 82*, 145–163, 1983.

[1062] M.J.B. ROBSHAW, "On evaluating the linear complexity of a sequence of least period 2^n", *Designs, Codes and Cryptography*, 4 (1994), 263–269.

[1063] ———, "Stream ciphers", Technical Report TR-701 (version 2.0), RSA Laboratories, 1995.

[1064] M. ROE, "How to reverse engineer an EES device", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 305–328, Springer-Verlag, 1995.

[1065] P. ROGAWAY, "Bucket hashing and its application to fast message authentication", *Advances in Cryptology–CRYPTO '95 (LNCS 963)*, 29–42, 1995.

[1066] P. ROGAWAY AND D. COPPERSMITH, "A software-optimized encryption algorithm", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 56–63, Springer-Verlag, 1994.

[1067] N. ROGIER AND P. CHAUVAUD, "The compression function of MD2 is not collision free", workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC'95), Ottawa, Canada, May 18–19 1995.

[1068] J. ROMPEL, "One-way functions are necessary and sufficient for secure signatures", *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, 387–394, 1990.

[1069] K.H. ROSEN, *Elementary Number Theory and its Applications*, Addison-Wesley, Reading, Massachusetts, 3rd edition, 1992.

[1070] J. ROSSER AND L. SCHOENFELD, "Approximate formulas for some functions of prime numbers", *Illinois Journal of Mathematics*, 6 (1962), 64–94.

[1071] RSA LABORATORIES, "The Public-Key Cryptography Standards – PKCS #11: Cryptographic token interface standard", RSA Data Security Inc., Redwood City, California, April 28 1995.

[1072] ———, "The Public-Key Cryptography Standards (PKCS)", RSA Data Security Inc., Redwood City, California, November 1993 Release.

[1073] A.D. RUBIN AND P. HONEYMAN, "Formal methods for the analysis of authentication protocols", CITI Technical Report 93-7, Information Technology Division, University of Michigan, 1993.

[1074] F. RUBIN, "Decrypting a stream cipher based on J-K flip-flops", *IEEE Transactions on Computers*, 28 (1979), 483–487.

[1075] R.A. RUEPPEL, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, 1986.

[1076] ———, "Correlation immunity and the summation generator", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 260–272, 1986.

[1077] ———, "Linear complexity and random sequences", *Advances in Cryptology–EUROCRYPT '85 (LNCS 219)*, 167–188, 1986.

[1078] ———, "Key agreements based on function composition", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 3–10, 1988.

[1079] ———, "On the security of Schnorr's pseudo random generator", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 423–428, 1990.

[1080] ———, "A formal approach to security architectures", *Advances in Cryptology–EUROCRYPT '91 (LNCS 547)*, 387–398, 1991.

[1081] ———, "Stream ciphers", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 65–134, IEEE Press, 1992.

[1082] ———, "Criticism of ISO CD 11166 banking — key management by means of asymmetric algorithms", W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy*, 191–198, 1993.

[1083] R.A. RUEPPEL, A. LENSTRA, M. SMID, K. MCCURLEY, Y. DESMEDT, A. ODLYZKO, AND P. LANDROCK, "The Eurocrypt '92 controversial issue: trapdoor primes and moduli", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 194–199, 1993.

[1084] R.A. RUEPPEL AND J.L. MASSEY, "The knapsack as a non-linear function", *IEEE International Symposium on Information Theory (Abstracts)*, p.46, 1985.

[1085] R.A. RUEPPEL AND O.J. STAFFELBACH, "Products of linear recurring sequences with maximum complexity", *IEEE Transactions on Information Theory*, 33 (1987), 124–131.

[1086] R.A. RUEPPEL AND P.C. VAN OORSCHOT, "Modern key agreement techniques", *Computer Communications*, 17 (1994), 458–465.

[1087] A. RUSSELL, "Necessary and sufficient conditions for collision-free hashing", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 433–441, 1993.

[1088] ———, "Necessary and sufficient conditions for collision-free hashing", *Journal of Cryptology*, 8 (1995), 87–99. An earlier version appeared in [1087].

[1089] A. SALOMAA, *Public-key Cryptography*, Springer-Verlag, Berlin, 1990.

[1090] M. SANTHA AND U.V. VAZIRANI, "Generating quasi-random sequences from slightly-random sources", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science*, 434–440, 1984.

[1091] ———, "Generating quasi-random sequences from semi-random sources", *Journal of Computer and System Sciences*, 33 (1986), 75–87. An earlier version appeared in [1090].

[1092] O. SCHIROKAUER, "Discrete logarithms and local units", *Philosophical Transactions of the Royal Society of London A*, 345 (1993), 409–423.

[1093] B. SCHNEIER, "Description of a new variable-length key, 64-bit block cipher (Blowfish)", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 191–204, Springer-Verlag, 1994.

[1094] ———, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, New York, 2nd edition, 1996.

[1095] C.P. SCHNORR, "Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system", U.S. Patent # 4,995,082, 19 Feb 1991.

[1096] ———, "On the construction of random number generators and random function generators", *Advances in Cryptology–EUROCRYPT '88 (LNCS 330)*, 225–232, 1988.

[1097] ———, "Efficient identification and signatures for smart cards", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 239–252, 1990.

[1098] ———, "Efficient signature generation by smart cards", *Journal of Cryptology*, 4 (1991), 161–174.

[1099] C.P. SCHNORR AND M. EUCHNER, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems", L. Budach, editor, *Fundamentals of Computation Theory (LNCS 529)*, 68–85, Springer-Verlag, 1991.

[1100] C.P. SCHNORR AND H.H. HÖRNER, "Attacking the Chor-Rivest cryptosystem by improved lattice reduction", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 1–12, 1995.

[1101] A. SCHÖNHAGE, "A lower bound for the length of addition chains", *Theoretical Computer Science*, 1 (1975), 1–12.

[1102] A.W. SCHRIFT AND A. SHAMIR, "On the universality of the next bit test", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 394–408, 1991.

[1103] ———, "Universal tests for nonuniform distributions", *Journal of Cryptology*, 6 (1993), 119–133. An earlier version appeared in [1102].

[1104] F. SCHWENK AND J. EISFELD, "Public key encryption and signature schemes based on polynomials over $\mathbb{Z}_n$", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 60–71, 1996.

[1105] R. SEDGEWICK, *Algorithms*, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1988.

[1106] R. SEDGEWICK, T.G. SZYMANSKI, AND A.C. YAO, "The complexity of finding cycles in periodic functions", *SIAM Journal on Computing*, 11 (1982), 376–390.

[1107] E.S. SELMER, "Linear recurrence relations over finite fields", Department of Mathematics, University of Bergen, Norway, 1966.

[1108] J. SHALLIT, "On the worst case of three algorithms for computing the Jacobi symbol", *Journal of Symbolic Computation*, 10 (1990), 593–610.

[1109] A. SHAMIR, "A fast signature scheme", MIT/LCS/TM-107, MIT Laboratory for Computer Science, 1978.

[1110] ———, "How to share a secret", *Communications of the ACM*, 22 (1979), 612–613.

[1111] ———, "On the generation of cryptographically strong pseudo-random sequences", S. Even and O. Kariv, editors, *Automata, Languages, and Programming, 8th Colloquium (LNCS 115)*, 544–550, Springer-Verlag, 1981.

[1112] ———, "On the generation of cryptographically strong pseudorandom sequences", *ACM Transactions on Computer Systems*, 1 (1983), 38–44. An earlier version appeared in [1111].

[1113] ———, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem", *Advances in Cryptology–Proceedings of Crypto 82*, 279–288, 1983.

[1114] ———, "A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem", *IEEE Transactions on Information Theory*, 30 (1984), 699–704. An earlier version appeared in [1113].

[1115] ———, "Identity-based cryptosystems and signature schemes", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 47–53, 1985.

[1116] ———, "An efficient identification scheme based on permuted kernels", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 606–609, 1990.

[1117] ———, "RSA for paranoids", *CryptoBytes*, 1 (Autumn 1995), 1–4.

[1118] A. SHAMIR AND A. FIAT, "Method, apparatus and article for identification and signature", U.S. Patent # 4,748,668, 31 May 1988.

[1119] M. SHAND AND J. VUILLEMIN, "Fast implementations of RSA cryptography", *Proceedings of the 11th IEEE Symposium on Computer Arithmetic*, 252–259, 1993.

[1120] C.E. SHANNON, "A mathematical theory of communication", *Bell System Technical Journal*, 27 (1948), 379–423, 623–656.

[1121] ———, "Communication theory of secrecy systems", *Bell System Technical Journal*, 28 (1949), 656–715.

[1122] ———, "Prediction and entropy of printed English", *Bell System Technical Journal*, 30 (1951), 50–64.

[1123] J. SHAWE-TAYLOR, "Generating strong primes", *Electronics Letters*, 22 (July 31, 1986), 875–877.

[1124] S. SHEPHERD, "A high speed software implementation of the Data Encryption Standard", *Computers & Security*, 14 (1995), 349–357.

[1125] A. SHIMIZU AND S. MIYAGUCHI, "Data randomization equipment", U.S. Patent # 4,850,019, 18 Jul 1989.

[1126] ———, "Fast data encipherment algorithm FEAL", *Advances in Cryptology–EUROCRYPT '87 (LNCS 304)*, 267–278, 1988.

[1127] Z. SHMUELY, "Composite Diffie-Hellman public-key generating systems are hard to break", Technical Report #356, TECHNION – Israel Institute of Technology, Computer Science Department, 1985.

[1128] P.W. SHOR, "Algorithms for quantum computation: discrete logarithms and factoring", *Proceedings of the IEEE 35th Annual Symposium on Foundations of Computer Science*, 124–134, 1994.

[1129] V. SHOUP, "New algorithms for finding irreducible polynomials over finite fields", *Mathematics of Computation*, 54 (1990), 435–447.

[1130] ———, "Searching for primitive roots in finite fields", *Mathematics of Computation*, 58 (1992), 369–380.

[1131] ———, "Fast construction of irreducible polynomials over finite fields", *Journal of Symbolic Computation*, 17 (1994), 371–391.

[1132] T. SIEGENTHALER, "Correlation-immunity of nonlinear combining functions for cryptographic applications", *IEEE Transactions on Information Theory*, 30 (1984), 776–780.

[1133] ———, "Decrypting a class of stream ciphers using ciphertext only", *IEEE Transactions on Computers*, 34 (1985), 81–85.

[1134] ———, "Cryptanalysts representation of nonlinearly filtered ML-sequences", *Advances in Cryptology–EUROCRYPT '85 (LNCS 219)*, 103–110, 1986.

[1135] R.D. SILVERMAN, "The multiple polynomial quadratic sieve", *Mathematics of Computation*, 48 (1987), 329–339.

[1136] R.D. SILVERMAN AND S.S. WAGSTAFF JR., "A practical analysis of the elliptic curve factoring algorithm", *Mathematics of Computation*, 61 (1993), 445–462.

[1137] G.J. SIMMONS, "A "weak" privacy protocol using the RSA crypto algorithm", *Cryptologia*, 7 (1983), 180–182.

[1138] ———, "Authentication theory/coding theory", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 411–431, 1985.

[1139] ———, "The subliminal channel and digital signatures", *Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209)*, 364–378, 1985.

[1140] ———, "A secure subliminal channel (?)", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 33–41, 1986.

[1141] ———, "How to (really) share a secret", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 390–448, 1990.

[1142] ———, "Prepositioned shared secret and/or shared control schemes", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 436–467, 1990.

[1143] ———, "Contemporary cryptology: a foreword", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, vii–xv, IEEE Press, 1992.

[1144] ———, "A survey of information authentication", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 379–419, IEEE Press, 1992.

[1145] ———, "An introduction to shared secret and/or shared control schemes and their application", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 441–497, IEEE Press, 1992.

[1146] ———, "How to insure that data acquired to verify treaty compliance are trustworthy", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 615–630, IEEE Press, 1992.

[1147] ———, "The subliminal channels in the U.S. Digital Signature Algorithm (DSA)", W. Wolfowicz, editor, *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy*, 35–54, 1993.

[1148] ———, "Proof of soundness (integrity) of cryptographic protocols", *Journal of Cryptology*, 7 (1994), 69–77.

[1149] ———, "Subliminal communication is easy using the DSA", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 218–232, 1994.

[1150] ———, "Protocols that ensure fairness", P.G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, 383–394, Institute of Mathematics & Its Applications (IMA), 1995.

[1151] G.J. SIMMONS AND M.J. NORRIS, "Preliminary comments on the M.I.T. public-key cryptosystem", *Cryptologia*, 1 (1977), 406–414.

[1152] A. SINKOV, *Elementary Cryptanalysis: A Mathematical Approach*, Random House, New York, 1968.

[1153] M.E. SMID, "Integrating the Data Encryption Standard into computer networks", *IEEE Transactions on Communications*, 29 (1981), 762–772.

[1154] M.E. SMID AND D.K. BRANSTAD, "Cryptographic key notarization methods and apparatus", U.S. Patent # 4,386,233, 31 May 1983.

[1155] ———, "The Data Encryption Standard: Past and future", *Proceedings of the IEEE*, 76 (1988), 550–559.

[1156] ———, "The Data Encryption Standard: Past and future", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 43–64, IEEE Press, 1992. Appeared earlier as [1155].

[1157] ———, "Response to comments on the NIST proposed digital signature standard", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 76–88, 1993.

[1158] D.R. SMITH AND J.T. PALMER, "Universal fixed messages and the Rivest-Shamir-Adleman cryptosystem", *Mathematika*, 26 (1979), 44–52.

[1159] J.L. SMITH, "Recirculating block cipher cryptographic system", U.S. Patent # 3,796,830, 12 Mar 1974.

[1160] ———, "The design of Lucifer: A cryptographic device for data communications", IBM Research Report RC 3326, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Apr. 15 1971.

[1161] P. SMITH AND M. LENNON, "LUC: A new public key system", E. Dougall, editor, *Proceedings of the IFIP TC11 Ninth International Conference on Information Security, IFIP/Sec 93*, 103–117, North-Holland, 1993.

[1162] P. SMITH AND C. SKINNER, "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 357–364, 1995.

[1163] R. SOLOVAY AND V. STRASSEN, "A fast Monte-Carlo test for primality", *SIAM Journal on Computing*, 6 (1977), 84–85. Erratum in ibid, 7 (1978), 118.

[1164] J. SORENSON, "Two fast gcd algorithms", *Journal of Algorithms*, 16 (1994), 110–144.

[1165] A. SORKIN, "Lucifer, a cryptographic algorithm", *Cryptologia*, 8 (1984), 22–35.

[1166] M. STADLER, J.-M. PIVETEAU, AND J. CAMENISCH, "Fair blind signatures", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 209–219, 1995.

[1167] O. STAFFELBACH AND W. MEIER, "Cryptographic significance of the carry for ciphers based on integer addition", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 601–614, 1991.

[1168] W. STAHNKE, "Primitive binary polynomials", *Mathematics of Computation*, 27 (1973), 977–980.

[1169] D.G. STEER, L. STRAWCZYNSKI, W. DIFFIE, AND M. WIENER, "A secure audio teleconference system", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 520–528, 1990.

[1170] J. STEIN, "Computational problems associated with Racah algebra", *Journal of Computational Physics*, 1 (1967), 397–405.

[1171] J.G. STEINER, C. NEUMAN, AND J.I. SCHILLER, "Kerberos: an authentication service for open network systems", *Proceedings of the Winter 1988 Usenix Conference*, 191–201, 1988.

[1172] M. STEINER, G. TSUDIK, AND M. WAIDNER, "Refinement and extension of encrypted key exchange", *Operating Systems Review*, 29:3 (1995), 22–30.

[1173] J. STERN, "Secret linear congruential generators are not cryptographically secure", *Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science*, 421–426, 1987.

[1174] ———, "An alternative to the Fiat-Shamir protocol", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 173–180, 1990.

[1175] ———, "Designing identification schemes with keys of short size", *Advances in Cryptology–CRYPTO '94 (LNCS 839)*, 164–173, 1994.

[1176] ———, "A new identification scheme based on syndrome decoding", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 13–21, 1994.

[1177] D.R. STINSON, "An explication of secret sharing schemes", *Designs, Codes and Cryptography*, 2 (1992), 357–390.

[1178] ———, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, Florida, 1995.

[1179] S.G. STUBBLEBINE AND V.D. GLIGOR, "On message integrity in cryptographic protocols", *Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, 85–104, 1992.

[1180] D.J. SYKES, "The management of encryption keys", D.K. Branstad, editor, *Computer security and the Data Encryption Standard*, 46–53, NBS Special Publication 500-27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.

[1181] P. SYVERSON, "Knowledge, belief and semantics in the analysis of cryptographic protocols", *Journal of Computer Security*, 1 (1992), 317–334.

[1182] ———, "A taxonomy of replay attacks", *Proceedings of the Computer Security Foundations Workshop VII (CSFW 1994)*, 187–191, IEEE Computer Society Press, 1994.

[1183] P. SYVERSON AND P. VAN OORSCHOT, "On unifying some cryptographic protocol logics", *Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy*, 14–28, 1994.

[1184] K. TANAKA AND E. OKAMOTO, "Key distribution using id-related information directory suitable for mail systems", *Proceedings of the 8th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'90)*, 115–122, 1990.

[1185] A. TARAH AND C. HUITEMA, "Associating metrics to certification paths", Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, editors, *Second European Symposium on Research in Computer Security – ESORICS'92 (LNCS 648)*, 175–189, Springer-Verlag, 1992.

[1186] J.J. TARDO AND K. ALAGAPPAN, "SPX: Global authentication using public key certificates", *Proceedings of the IEEE Symposium on Research in Security and Privacy*, 232–244, 1991.

[1187] A. TARDY-CORFDIR AND H. GILBERT, "A known plaintext attack of FEAL-4 and FEAL-6", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 172–182, 1992.

[1188] M. TATEBAYASHI, N. MATSUZAKI, AND D.B. NEWMAN JR., "Key distribution protocol for digital mobile communication systems", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 324–334, 1990.

[1189] R. TAYLOR, "An integrity check value algorithm for stream ciphers", *Advances in Cryptology–CRYPTO '93 (LNCS 773)*, 40–48, 1994.

[1190] J.A. THIONG LY, "A serial version of the Pohlig-Hellman algorithm for computing discrete logarithms", *Applicable Algebra in Engineering, Communication and Computing*, 4 (1993), 77–80.

[1191] J. THOMPSON, "S/MIME message specification – PKCS security services for MIME", RSA Data Security Inc., Aug. 29 1995, `http://www.rsa.com/`.

[1192] T. TOKITA, T. SORIMACHI, AND M. MATSUI, "Linear cryptanalysis of LOKI and s^2DES", *Advances in Cryptology–ASIACRYPT '94 (LNCS 917)*, 293–303, 1995.

[1193] ———, "On applicability of linear cryptanalysis to DES-like cryptosystems – LOKI89, LOKI91 and s^2DES", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, E78-A (1995), 1148–1153. An earlier version appeared in [1192].

[1194] M. TOMPA AND H. WOLL, "Random self-reducibility and zero-knowledge interactive proofs of possession of information", *Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science*, 472–482, 1987.

[1195] ———, "How to share a secret with cheaters", *Journal of Cryptology*, 1 (1988), 133–138.

[1196] G. TSUDIK, "Message authentication with one-way hash functions", *Computer Communication Review*, 22 (1992), 29–38.

[1197] S. TSUJII AND J. CHAO, "A new ID-based key sharing system", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 288–299, 1992.

[1198] W. TUCHMAN, "Integrated system design", D.K. Branstad, editor, *Computer security and the Data Encryption Standard*, 94–96, NBS Special Publication 500-27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.

[1199] ———, "Hellman presents no shortcut solutions to the DES", *IEEE Spectrum*, 16 (1979), 40–41.

[1200] J. VAN DE GRAAF AND R. PERALTA, "A simple and secure way to show the validity of your public key", *Advances in Cryptology–CRYPTO '87 (LNCS 293)*, 128–134, 1988.

[1201] E. VAN HEIJST AND T.P. PEDERSEN, "How to make efficient fail-stop signatures", *Advances in Cryptology–EUROCRYPT '92 (LNCS 658)*, 366–377, 1993.

[1202] E. VAN HEIJST, T.P. PEDERSEN, AND B. PFITZMANN, "New constructions of fail-stop signatures and lower bounds", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 15–30, 1993.

[1203] P. VAN OORSCHOT, "A comparison of practical public key cryptosystems based on integer factorization and discrete logarithms", G.J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, 289–322, IEEE Press, 1992.

[1204] ———, "Extending cryptographic logics of belief to key agreement protocols", *1st ACM Conference on Computer and Communications Security*, 232–243, ACM Press, 1993.

[1205] ———, "An alternate explanation of two BAN-logic "failures"", *Advances in Cryptology–EUROCRYPT '93 (LNCS 765)*, 443–447, 1994.

[1206] P. VAN OORSCHOT AND M. WIENER, "A known-plaintext attack on two-key triple encryption", *Advances in Cryptology–EUROCRYPT '90 (LNCS 473)*, 318–325, 1991.

[1207] ———, "Parallel collision search with applications to hash functions and discrete logarithms", *2nd ACM Conference on Computer and Communications Security*, 210–218, ACM Press, 1994.

[1208] ———, "Improving implementable meet-in-the-middle attacks by orders of magnitude", *Advances in Cryptology–CRYPTO '96 (LNCS 1109)*, 229–236, 1996.

[1209] ———, "On Diffie-Hellman key agreement with short exponents", *Advances in Cryptology–EUROCRYPT '96 (LNCS 1070)*, 332–343, 1996.

[1210] H.C.A. VAN TILBORG, *An Introduction to Cryptology*, Kluwer Academic Publishers, Boston, 1988.

[1211] ———, "Authentication codes: an area where coding and cryptology meet", C. Boyd, editor, *Cryptography and Coding, 5th IMA Conference, Proceedings*, 169–183, Institute of Mathematics & Its Applications (IMA), 1995.

[1212] J. VAN TILBURG, "On the McEliece public-key cryptosystem", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 119–131, 1990.

[1213] S.A. VANSTONE AND R.J. ZUCCHERATO, "Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbb{Z}_n$", *IEEE Transactions on Information Theory*, to appear.

[1214] ———, "Short RSA keys and their generation", *Journal of Cryptology*, 8 (1995), 101–114.

[1215] S. VAUDENAY, "On the need for multipermutations: Cryptanalysis of MD4 and SAFER", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 286–297, Springer-Verlag, 1995.

[1216] ———, "On the weak keys of Blowfish", D. Gollmann, editor, *Fast Software Encryption, Third International Workshop (LNCS 1039)*, 27–32, Springer-Verlag, 1996.

[1217] U.V. VAZIRANI, "Towards a strong communication complexity theory, or generating quasi-random sequences from two communicating slightly-random sources", *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, 366–378, 1985.

[1218] U.V. VAZIRANI AND V.V. VAZIRANI, "Efficient and secure pseudo-random number generation", *Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science*, 458–463, 1984. This paper also appeared in [1219].

[1219] ———, "Efficient and secure pseudo-random number generation", *Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196)*, 193–202, 1985.

[1220] K. VEDDER, "Security aspects of mobile communications", B. Preneel, R. Govaerts, and J. Vandewalle, editors, *Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741)*, 193–210, Springer-Verlag, 1993.

[1221] G.S. VERNAM, "Secret signaling system", U.S. Patent # 1,310,719, 22 Jul 1919.

[1222] ———, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", *Journal of the American Institute for Electrical Engineers*, 55 (1926), 109–115.

[1223] J. VON NEUMANN, "Various techniques used in connection with random digits", *Applied Mathematics Series, U.S. National Bureau of Standards*, 12 (1951), 36–38.

[1224] J. VON ZUR GATHEN AND V. SHOUP, "Computing Frobenius maps and factoring polynomials", *Computational Complexity*, 2 (1992), 187–224.

[1225] V.L. VOYDOCK AND S.T. KENT, "Security mechanisms in high-level network protocols", *Computing Surveys*, 15 (1983), 135–171.

[1226] D. WACKERLY, W. MENDENHALL III, AND R. SCHEAFFER, *Mathematical Statistics with Applications*, Duxbury Press, Belmont, California, 5th edition, 1996.

[1227] M. WAIDNER AND B. PFITZMANN, "The dining cryptographers in the disco: Unconditional sender and recipient untraceability with computationally secure serviceability", *Advances in Cryptology–EUROCRYPT '89 (LNCS 434)*, 690, 1990.

[1228] C.P. WALDVOGEL AND J.L. MASSEY, "The probability distribution of the Diffie-Hellman key", *Advances in Cryptology–AUSCRYPT '92 (LNCS 718)*, 492–504, 1993.

[1229] S.T. WALKER, S.B. LIPNER, C.M. ELLISON, AND D.M. BALENSON, "Commercial key recovery", *Communications of the ACM*, 39 (1996), 41–47.

[1230] C.D. WALTER, "Faster modular multiplication by operand scaling", *Advances in Cryptology–CRYPTO '91 (LNCS 576)*, 313–323, 1992.

[1231] P.C. WAYNER, "Content-addressable search engines and DES-like systems", *Advances in Cryptology–CRYPTO '92 (LNCS 740)*, 575–586, 1993.

[1232] D. WEBER, "An implementation of the general number field sieve to compute discrete logarithms mod p", *Advances in Cryptology–EUROCRYPT '95 (LNCS 921)*, 95–105, 1995.

[1233] A.F. WEBSTER AND S.E. TAVARES, "On the design of S-boxes", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 523–534, 1986.

[1234] M.N. WEGMAN AND J.L. CARTER, "New hash functions and their use in authentication and set equality", *Journal of Computer and System Sciences*, 22 (1981), 265–279.

[1235] D. WELSH, *Codes and Cryptography*, Clarendon Press, Oxford, 1988.

[1236] A.E. WESTERN AND J.C.P. MILLER, *Tables of Indices and Primitive Roots*, volume 9, Royal Society Mathematical Tables, Cambridge University Press, 1968.

[1237] D.J. WHEELER, "A bulk data encryption algorithm", R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop (LNCS 809)*, 127–134, Springer-Verlag, 1994.

[1238] D.J. WHEELER AND R.M. NEEDHAM, "TEA, a tiny encryption algorithm", B. Preneel, editor, *Fast Software Encryption, Second International Workshop (LNCS 1008)*, 363–366, Springer-Verlag, 1995.

[1239] D.H. WIEDEMANN, "Solving sparse linear equations over finite fields", *IEEE Transactions on Information Theory*, 32 (1986), 54–62.

[1240] M.J. WIENER, "Cryptanalysis of short RSA secret exponents", *IEEE Transactions on Information Theory*, 36 (1990), 553–558.

[1241] ———, "Efficient DES key search", Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, 1994. Presented at Crypto '93 rump session.

[1242] S. WIESNER, "Conjugate coding", *SIGACT News*, 15 (1983), 78–88. Original manuscript (*circa* 1970).

[1243] H.S. WILF, "Backtrack: An O(1) expected time algorithm for the graph coloring problem", *Information Processing Letters*, 18 (1984), 119–121.

[1244] M.V. WILKES, *Time-Sharing Computer Systems*, American Elsevier Pub. Co., New York, 3rd edition, 1975.

[1245] F. WILLEMS, "Universal data compression and repetition times", *IEEE Transactions on Information Theory*, 35 (1989), 54–58.

[1246] H.C. WILLIAMS, "A modification of the RSA public-key encryption procedure", *IEEE Transactions on Information Theory*, 26 (1980), 726–729.

[1247] ———, "A $p+1$ method of factoring", *Mathematics of Computation*, 39 (1982), 225–234.

[1248] ———, "Some public-key crypto-functions as intractable as factorization", *Cryptologia*, 9 (1985), 223–237.

[1249] H.C. WILLIAMS AND B. SCHMID, "Some remarks concerning the M.I.T. public-key cryptosystem", *BIT*, 19 (1979), 525–538.

[1250] R.S. WINTERNITZ, "A secure one-way hash function built from DES", *Proceedings of the 1984 IEEE Symposium on Security and Privacy*, 88–90, 1984.

[1251] S. WOLFRAM, "Cryptography with cellular automata", *Advances in Cryptology–CRYPTO '85 (LNCS 218)*, 429–432, 1986.

[1252] ———, "Random sequence generation by cellular automata", *Advances in Applied Mathematics*, 7 (1986), 123–169.

[1253] H. WOLL, "Reductions among number theoretic problems", *Information and Computation*, 72 (1987), 167–179.

[1254] A.D. WYNER, "The wire-tap channel", *Bell System Technical Journal*, 54 (1975), 1355–1387.

[1255] Y. YACOBI, "A key distribution "paradox"", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 268–273, 1991.

[1256] Y. YACOBI AND Z. SHMUELY, "On key distribution systems", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 344–355, 1990.

[1257] A.C. YAO, "On the evaluation of powers", *SIAM Journal on Computing*, 5 (1976), 100–103.

[1258] ———, "Theory and applications of trapdoor functions", *Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science*, 80–91, 1982.

[1259] S.-M. YEN AND C.-S. LAIH, "New digital signature scheme based on discrete logarithm", *Electronics Letters*, 29 (June 10, 1993), 1120–1121.

[1260] C. YUEN, "Testing random number generators by Walsh transform", *IEEE Transactions on Computers*, 26 (1977), 329–333.

[1261] D. YUN, "Fast algorithm for rational function integration", *Information Processing 77: Proceedings of IFIP Congress 77*, 493–498, 1977.

[1262] G. YUVAL, "How to swindle Rabin", *Cryptologia*, 3 (1979), 187–190.

[1263] K. ZENG AND M. HUANG, "On the linear syndrome method in cryptanalysis", *Advances in Cryptology–CRYPTO '88 (LNCS 403)*, 469–478, 1990.

[1264] K. ZENG, C.-H. YANG, AND T.R.N. RAO, "On the linear consistency test (LCT) in cryptanalysis with applications", *Advances in Cryptology–CRYPTO '89 (LNCS 435)*, 164–174, 1990.

[1265] ———, "An improved linear syndrome algorithm in cryptanalysis with applications", *Advances in Cryptology–CRYPTO '90 (LNCS 537)*, 34–47, 1991.

[1266] K. ZENG, C.-H. YANG, D.-Y WEI, AND T.R.N. RAO, "Pseudorandom bit generators in stream-cipher cryptography", *Computer*, 24 (1991), 8–17.

[1267] C. ZHANG, "An improved binary algorithm for RSA", *Computers and Mathematics with Applications*, 25:6 (1993), 15–24.

[1268] Y. ZHENG, J. PIEPRZYK, AND J. SEBERRY, "HAVAL – a one-way hashing algorithm with variable length of output", *Advances in Cryptology–AUSCRYPT '92 (LNCS 718)*, 83–104, 1993.

[1269] Y. ZHENG AND J. SEBERRY, "Immunizing public key cryptosystems against chosen ciphertext attacks", *IEEE Journal on Selected Areas in Communications*, 11 (1993), 715–724.

[1270] N. ZIERLER, "Primitive trinomials whose degree is a Mersenne exponent", *Information and Control*, 15 (1969), 67–69.

[1271] N. ZIERLER AND J. BRILLHART, "On primitive trinomials (mod 2)", *Information and Control*, 13 (1968), 541–554.

[1272] P.R. ZIMMERMANN, *The Official PGP User's Guide*, MIT Press, Cambridge, Massachusetts, 1995 (second printing).

[1273] J. ZIV AND A. LEMPEL, "On the complexity of finite sequences", *IEEE Transactions on Information Theory*, 22 (1976), 75–81.

[1274] M. ŽIVKOVIĆ, "An algorithm for the initial state reconstruction of the clock-controlled shift register", *IEEE Transactions on Information Theory*, 37 (1991), 1488–1490.

[1275] ———, "A table of primitive binary polynomials", *Mathematics of Computation*, 62 (1994), 385–386.

[1276] ———, "Table of primitive binary polynomials. II", *Mathematics of Computation*, 63 (1994), 301–306.