Bibliography

[ACGS88] W. Alexi, B. Chor, O. Goldreich and C. P. Schnorr. RSA and Rabin functions: certain parts are as hard as the whole. *SIAM Jounal on Computing*, **17** (1988), 194–209.

[An91] H. Anton. *Elementary Linear Algebra* (Sixth Edition). John Wiley and Sons, 1991.

[BHS93] D. Bayer, S. Haber and W. S. Stornetta. Improving the efficiency and reliability of digital time-stamping. In *Sequences II, Methods in Communication, Security, and Computer Science*, pages 329–334. Springer-Verlag, 1993.

[BB88] P. Beauchemin and G. Brassard. A generalization of Hellman's extension to Shannon's approach to cryptography. *Journal of Cryptology*, **1** (1988), 129–131.

[BBCGP88] 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.

[BC94] A. Beimel and B. Chor. Interaction in key distribution schemes. *Lecture Notes in Computer Science*, **773** (1994), 444–455. (Advances in Cryptology – CRYPTO '93.)

[BP82] H. Beker and F. Piper. *Cipher Systems, The Protection of Communications*. John Wiley and Sons, 1982.

[BL90] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. *Lecture Notes in Computer Science*, **403** (1990), 27–35. (Advances in Cryptology – CRYPTO '88.)

[Be83] T. Beth (Ed.) *Cryptography Proceedings, 1982. Lecture Notes in Computer Science*, vol. 149, Springer-Verlag, 1983.

[BCI85] T. Beth, N. Cot and I. Ingemarsson (Eds.) *Advances in Cryptology: Proceedings of EUROCRYPT '84. Lecture Notes in Computer Science*, vol. 209, Springer-Verlag, 1985.

[BJL85] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Bibliographisches Institut, Zurich, 1985.

[Be94] A. Beutelspacher. *Cryptology*. Mathematical Association of America, 1994.

[BS91] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, **4** (1991), 3–72.

[BS93] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard.* Springer-Verlag, 1993.

[BS93a] E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. *Lecture Notes in Computer Science*, **740** (1993), 494–502. (Advances in Cryptology – CRYPTO '92.)

[Bl79] G. R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, **48** (1979), 313–317.

[BC85] G. R. Blakley and D. Chaum (Eds.) *Advances in Cryptology: Proceedings of CRYPTO '84. Lecture Notes in Computer Science*, vol. 196, Springer-Verlag, 1985.

[Bl85] R. Blom An optimal class of symmetric key generation schemes. *Lecture Notes in Computer Science*, **209** (1985), 335–338. (Advances in Cryptology – EUROCRYPT '84.)

[BBS86] L. Blum, M. Blum and M. Shub. A simple unpredictable random number generator. *SIAM Jounal on Computing*, **15** (1986), 364–383.

[Bl82] M. Blum. Coin flipping by telephone: a protocol for solving impossible problems In *24th IEEE Spring Computer Conference*, pages 133–137. IEEE Press, 1982.

[BG85] M. Blum and S. Goldwasser. An efficient probabilistic public-key cryptosystem that hides all partial information. *Lecture Notes in Computer Science*, **196** (1985), 289–302. (Advances in Cryptology – CRYPTO '84.)

[BM84] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Jounal on Computing*, **13** (1984), 850–864.

[Bo89] J. Boyar. Inferring sequences produced by pseudo-random number generators. *Journal of Association for Computing Machinery*, **36** (1989), 129–141.

[BDSV93] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *Lecture Notes in Computer Science*, **658** (1993), 1–24. (Advances in Cryptology – EUROCRYPT '92.)

[BDSHKVY93] C. Blundo, A. De Santis,A. Herzberg, S. Kutten, U. Vaccaro and M. Yung. Perfectly-secure key distribution for dynamic conferences. *Lecture Notes in Computer Science*, **740**

(1993), 471–486. (Advances in Cryptology – CRYPTO '92.)

[BC93] J. N. E. Bos and D. Chaum. Provably unforgeable signatures. *Lecture Notes in Computer Science*, **740** (1993), 1–14. (Advances in Cryptology – CRYPTO '92.)

[Br88] G. Brassard. *Modern Cryptology – A Tutorial. Lecture Notes in Computer Science*, vol. 325, Springer-Verlag, 1988.

[Br90] G. Brassard (Ed.) *Advances in Cryptology – CRYPTO '89 Proceedings. Lecture Notes in Computer Science*, vol. 435, Springer-Verlag, 1990.

[BB88a] G. Brassard and P. Bratley. *Algorithmics, Theory and Practice*. Prentice Hall, 1988.

[BCC88] G. Brassard, D. Chaum and C. Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and Systems Science*, **37** (1988), 156–189.

[BC90] G. Brassard and C. Crépeau. Sorting out zero-knowledge. *Lecture Notes in Computer Science*, **434** (1990), 181–191. (Advances in Cryptology – EUROCRYPT '89.)

[Br89] D. M. Bressoud. *Factorization and Primality Testing*. Springer-Verlag, 1989.

[Br85] E. F. Brickell. Breaking iterated knapsacks. *Lecture Notes in Computer Science*, **218** (1986), 342–358. (Advances in Cryptology – CRYPTO '85.)

[Br89a] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, **9** (1989), 105–113.

[Br93] E. F. Brickell (Ed.) *Advances in Cryptology – CRYPTO '92 Proceedings. Lecture Notes in Computer Science*, vol. 740, Springer-Verlag, 1993.

[BD91] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, **4** (1991), 123–134.

[BM92] E. F. Brickell and K. S. McCurley. An interactive identification scheme based on discrete logarithms and factoring. *Journal of Cryptology*, **5** (1992), 29–39.

[BMP87] E. F. Brickell, J. H. Moore and M. R. Purtill. Structure in the S-boxes of DES. *Lecture Notes in Computer Science*, **263** (1987), 3–8. (Advances in Cryptology – CRYPTO '86.)

[BO92] E. F. Brickell and A. M. Odlyzko. Cryptanalysis, a survey of recent results. In *Contemporary Cryptology, The Science of Information Integrity*, pages 501–540. IEEE Press, 1992.

[BS92] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *Journal of Cryptology*, **5** (1992), 153–166.

[BKPS90] L. Brown, M. Kwan, J. Pieprzyk and J. Seberry. LOKI – A cryptographic primitive for authentication and secrecy applications. *Lecture Notes in Computer Science*, **453** (1990), 229–236. (Advances in Cryptology – AUSCRYPT '90.)

[BDB92] M. Burmester, Y. Desmedt and T. Beth. Efficient zero-knowledge identification schemes for smart cards. *The Computer Journal*, **35** (1992), 21–29.

[CDGV93] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *Journal of Cryptology*, **6** (1993), 157–167.

[CH95] F. Chabaud. On the security of some cryptosystems based on error-correcting codes. *Lecture Notes in Computer Science*, to appear. (Advances in Cryptology – EUROCRYPT '94.)

[CH84] D. Chaum (Ed.) *Advances in Cryptology: Proceedings of CRYPTO '83.* Plenum Press, 1984.

[CP88] D. Chaum and W. L. Price (Eds.) *Advances in Cryptology – EUROCRYPT '87 Proceedings. Lecture Notes in Computer Science*, vol. 304, Springer-Verlag, 1988.

[CRS83] D. Chaum, R. L. Rivest and A. T. Sherman (Eds.) *Advances in Cryptology: Proceedings of CRYPTO '82.* Plenum Press, 1983.

[CvA90] D. Chaum and H. van Antwerpen. Undeniable signatures. *Lecture Notes in Computer Science*, **435** (1990), 212–216. (Advances in Cryptology – CRYPTO '89.)

[CvHP92] D. Chaum, E. van Heijst and B. Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer. *Lecture Notes in Computer Science*, **576** (1992), 470–484. (Advances in Cryptology – CRYPTO '91.)

[CR88] B. Chor and R. L. Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, **45** (1988), 901–909.

[CKM94] D. Coppersmith, H. Krawczyz and Y. Mansour. The shrinking generator. *Lecture Notes in Computer Science*, **773** (1994), 22–39. (Advances in Cryptology – CRYPTO '93.)

[CSV94] D. Coppersmith, J. Stern and S. Vaudenay. Attacks on the birational permutation signature schemes. *Lecture Notes in Computer Science*, **773** (1994), 435–443. (Advances in Cryptology – CRYPTO '93.)

[CW91] T. W. CUSICK AND M. C. WOOD. The REDOC-II cryptosystem. *Lecture Notes in Computer Science*, **537** (1991), 545–563. (Advances in Cryptology – CRYPTO '90.)

[DA90] I. B. DÅMGARD. A design principle for hash functions. *Lecture Notes in Computer Science*, **435** (1990), 416–427. (Advances in Cryptology – CRYPTO '89.)

[DA91] I. B. DÅMGARD (ED.) *Advances in Cryptology – EUROCRYPT '90 Proceedings. Lecture Notes in Computer Science*, vol. 473, Springer-Verlag, 1991.

[DLP93] I. DÅMGARD, P. LANDROCK AND C. POMERANCE. Average case error estimates for the strong probable prime test. *Mathematics of Computation*, **61** (1993), 177–194.

[DA91A] D. W. DAVIES (ED.) *Advances in Cryptology – EUROCRYPT '91 Proceedings. Lecture Notes in Computer Science*, vol. 547, Springer-Verlag, 1991.

[DE84] J. M. DELAURENTIS. A further weakness in the common modulus protocol for the RSA cryptosystem. *Cryptologia*, **8** (1984), 253–259.

[DBB92] B. DEN BOER AND A. BOSSALAERS. An attack on the last two rounds of MD4. *Lecture Notes in Computer Science*, **576** (1992), 194–203. (Advances in Cryptology – CRYPTO '91.)

[DE82] D. E. R. DENNING. *Cryptography and Data Security*. Addison-Wesley, 1982.

[DE94] Y. G. DESMEDT (ED.) *Advances in Cryptology – CRYPTO '94 Proceedings. Lecture Notes in Computer Science*, vol. 839, Springer-Verlag, 1994.

[DWQ93] D. DE WALEFFE AND J.-J. QUISQUATER. Better login protocols for computer networks. *Lecture Notes in Computer Science*, **741** (1993), 50–70. (Computer Security and Industrial Cryptography, State of the Art and Evolution, ESAT Course, May 1991.)

[DI92] W. DIFFIE. The first ten years of public-key cryptography. In *Contemporary Cryptology, The Science of Information Integrity*, pages 135–175. IEEE Press, 1992.

[DH76] W. DIFFIE AND M. E. HELLMAN. Multiuser cryptographic techniques. *AFIPS Conference Proceedings*, **45** (1976), 109–112.

[DH76A] W. DIFFIE AND M. E. HELLMAN. New directions in cryptography. *IEEE Transactions on Information Theory*, **22** (1976), 644–654.

[DVW92] W. DIFFIE, P. C. VAN OORSCHOT AND M. J. WIENER. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, **2** (1992), 107–125.

[EB93] H. EBERLE. A high-speed DES implementation for network applications. *Lecture Notes in Computer Science*, **740** (1993), 527–545. (Advances in Cryptology – CRYPTO '92.)

[EL85] T. ELGAMAL. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **31** (1985), 469–472.

[EAKMM86] D. ESTES, L. M. ADLEMAN, K. KOMPELLA, K. S. MCCURLEY AND G. L. MILLER. Breaking the Ong-Schnorr-Shamir signature schemes for quadratic number fields. *Lecture Notes in Computer Science*, **218** (1986), 3–13. (Advances in Cryptology – CRYPTO '85.)

[FFS88] U. FEIGE, A. FIAT AND A. SHAMIR. Zero-knowledge proofs of identity. *Journal of Cryptology*, **1** (1988), 66–94.

[FE92] J. FEIGENBAUM (ED.) *Advances in Cryptology – CRYPTO '91 Proceedings. Lecture Notes in Computer Science*, vol. 576, Springer-Verlag, 1992.

[FE73] H. FEISTEL. Cryptography and computer privacy. *Scientific American*, **228**(5) (1973), 15–23.

[FN91] A. FIAT AND M. NAOR. Rigorous time/space trade-offs for inverting functions. In *Proceedings of the 23rd Symposium on the Theory of Computing*, pages 534–541. ACM Press, 1991.

[FS87] A. FIAT AND A. SHAMIR. How to prove yourself: practical solutions to identification and signature problems. *Lecture Notes in Computer Science*, **263** (1987), 186–194. (Advances in Cryptology – CRYPTO '86.)

[FOM91] A. FUJIOKA, T. OKAMOTO AND S. MIYAGUCHI. ESIGN: an efficient digital signature implementation for smart cards. *Lecture Notes in Computer Science*, **547** (1991), 446–457. (Advances in Cryptology – EUROCRYPT '91.)

[GIB91] J. K. GIBSON. Discrete logarithm hash function that is collision free and one way. *IEE Proceedings-E*, **138** (1991), 407–410.

[GMS74] E. N. GILBERT, F. J. MACWILLIAMS AND N. J. A. SLOANE. Codes which detect deception. *Bell Systems Technical Journal*, **53** (1974), 405–424.

[GIR91] M. GIRAULT. Self-certified public keys. *Lecture Notes in Computer Science*, **547** (1991), 490–497. (Advances in Cryptology – EUROCRYPT '91.)

[GP91] C. M. GOLDIE AND R. G. E. PINCH. *Communication Theory*.

Cambridge University Press, 1991.

[GMW91] O. Goldreich, A. Micali and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, **38** (1991), 691–729.

[Go90] S. Goldwasser (Ed.) *Advances in Cryptology – CRYPTO '88 Proceedings. Lecture Notes in Computer Science*, vol. 403, Springer-Verlag, 1990.

[GM84] S. Goldwasser and A. Micali. Probabilistic encryption. *Journal of Computer and Systems Science*, **28** (1984), 270–299.

[GMR89] S. Goldwasser, S. Micali and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, **18** (1989), 186–208.

[GMT82] S. Goldwasser, S. Micali and P. Tong. Why and how to establish a common code on a public network. In *23rd Annual Symposium on the Foundations of Computer Science*, pages 134–144. IEEE Press, 1982.

[GM93] D. M. Gordon and K. S. McCurley. Massively parallel computation of discrete logarithms. *Lecture Notes in Computer Science*, **740** (1993), 312–323. (Advances in Cryptology – CRYPTO '92.)

[GQ88] L. C. Guillou and J.-J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. *Lecture Notes in Computer Science*, **330** (1988), 123–128. (Advances in Cryptology – EUROCRYPT '88.)

[Gu88] C. G. Gunther Alternating step generators controlled by de Bruijn sequences. *Lecture Notes in Computer Science*, **304** (1988), 88–92. (Advances in Cryptology – EUROCRYPT '87.)

[Gu88a] C. G. Gunther (Ed.) *Advances in Cryptology – EUROCRYPT '88 Proceedings. Lecture Notes in Computer Science*, vol. 330, Springer-Verlag, 1988.

[HS91] S. Haber and W. S. Stornetta. How to timestamp a digital document. *Journal of Cryptology*, **3** (1991), 99–111.

[HSS93] J. Håstad, A. W. Schrift and A. Shamir. The discrete logarithm modulo a composite hides $O(n)$ bits. *Journal of Computer and Systems Science*, **47** (1993), 376–404.

[He80] M. E. Hellman. A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory*, **26** (1980), 401–

406.

[Hi29] L. S. Hill. Cryptogaphy in an algebraic alphabet. *American Mathematical Monthly*, **36** (1929), 306–312.

[He94] T. Helleseth (Ed.) *Advances in Cryptology – EUROCRYPT '93 Proceedings. Lecture Notes in Computer Science*, vol. 765, Springer-Verlag, 1994.

[HLLPRW91] D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger and J. R. Wall. *Coding Theory, The Essentials*. Marcel Dekker, 1991.

[IRM93] H. Imai, R. L. Rivest and T. Matsumoto (Eds.) *Advances in Cryptology – ASIACRYPT '91 Proceedings. Lecture Notes in Computer Science*, vol. 739, Springer-Verlag, 1993.

[ISN87] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *Proceedings IEEE Globecom '87*, pages 99–102, 1987.

[Jo88] D. S. Johnson. The NP-completeness column: an ongoing guide. *Journal of Algorithms*, **9** (1988), 426–444.

[Ka67] D. Kahn. *The Codebreakers. The Story of Secret Writing*. Macmillan, 1967.

[Ko87] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag, 1987.

[Ko87a] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, **48** (1987), 203–209.

[Ko87a] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, **48** (1987), 203–209.

[KN93] J. Kohl and C. Neuman. *The Kerboros Network Authentication Service*. Network Working Group Request for Comments: 1510, September 1993.

[Ko81] A. G. Konheim. *Cryptography, A Primer*. John Wiley and Sons, 1981.

[Kr86] E. Kranakis. *Primality and Cryptography*. John Wiley and Sons, 1986.

[La90] J. C. Lagarias Pseudo-random number generators in cryptography and number theory. In *Cryptology and Computational Number Theory*, pages 115–143. American Mathematical Society, 1990.

[LO91] B. A. LaMacchia and A. M. Odlyzko. Computation of discrete logarithms in finite fields. *Designs, Codes and Cryptography*, **1** (1991), 47–62.

[LL93] A. K. Lenstra and H. W. Lenstra, Jr. (Eds.) *The Develop-*

ment of the Number Field Sieve. Lecture Notes in Mathematics, vol. 1554. Springer-Verlag, 1993.

[LL90] A. K. Lenstra and H. W. Lenstra, Jr. Algorithms in number theory. In *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity*, pages 673–715. Elsevier Science Publishers, 1990.

[LN83] R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley, 1983.

[LW88] D. L. Long and A. Wigderson. The discrete log hides $O(\log n)$ bits. *SIAM Joumal on Computing*, **17** (1988), 363–372.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[Ma86] J. L. Massey. Cryptography – a selective survey. In *Digital Communications*, pages 3–21. North-Holland, 1986.

[Ma94] M. Matsui. Linear cryptanalysis method for DES cipher. *Lecture Notes in Computer Science*, **765** (1994), 386–397. (Advances in Cryptology – EUROCRYPT '93.)

[Ma94a] M. Matsui. The first experimental cryptanalysis of the data encryption standard. *Lecture Notes in Computer Science*, **839** (1994), 1–11. (Advances in Cryptology – CRYPTO '94.)

[MTI86] T. Matsumoto, Y. Takashima and H. Imai. On seeking smart public-key distribution systems. *Transactions of the IECE (Japan)*, **69** (1986), 99–106.

[Mc90] K. McCurley The discrete logarithm problem. In *Cryptology and Computational Number Theory*, pages 49–74. American Mathematical Society, 1990.

[Mc78] R. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, **42–44** (1978), 114–116.

[Mc87] R. McEliece. *Finite Fields for Computer Scientists and Engineers.* Kluwer Academic Publishers, 1987.

[Me93] A. J. Menezes. *Elliptic Curve Public Key Cryptosystems.* Kluwer Academic Publishers, 1993.

[MBGMVY93] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian. *Applications of Finite Fields.* Kluwer Academic Publishers, 1993.

[MOV94] A. J. Menezes, T. Okamoto and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, **39** (1993), 1639–1646.

[MV91] A. J. Menezes and S. A. Vanstone (Eds.) *Advances in Cryp-*

Previous Chapter Previous Page Home Next page

tology – CRYPTO '90 Proceedings. Lecture Notes in Computer Science, vol. 537, Springer-Verlag, 1991.

[MV93] A. J. Menezes and S. A. Vanstone. Elliptic curve cryptosystems and their implementation. *Journal of Cryptology*, **6** (1993), 209–224.

[Me78] R. C. Merkle. Secure communications over insecure channels. *Communications of the ACM*, **21** (1978), 294–299.

[Me90] R. C. Merkle. One way hash functions and DES. *Lecture Notes in Computer Science*, **435** (1990), 428–446. (Advances in Cryptology – CRYPTO '89.)

[Me90a] R. C. Merkle. A fast software one-way hash function. *Journal of Cryptology*, **3** (1990), 43–58.

[MH78] R. C. Merkle and M. E. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, **24** (1978), 525–530.

[MM82] C. Meyer and S. Matyas. *Cryptography: A New Dimension in Computer Security*. John Wiley and Sons, 1982.

[Mi76] G. L. Miller. Riemann's hypothesis and tests for primality. *Journal of Computer and Systems Science*, **13** (1976), 300–317.

[Mi86] V. Miller. Uses of elliptic curves in cryptography. *Lecture Notes in Computer Science*, **218** (1986), 417–426. (Advances in Cryptology – CRYPTO '85.)

[MPW92] C. J. Mitchell, F. Piper and P. Wild. Digital signatures. In *Contemporary Cryptology, The Science of Information Integrity*, pages 325–378. IEEE Press, 1992.

[Mi91] S. Miyaguchi. The FEAL cipher family. *Lecture Notes in Computer Science*, **537** (1991), 627–638. (Advances in Cryptology – CRYPTO '90.)

[MOI90] S. Miyaguchi, K. Ohta and M. Iwata. 128-bit hash function (N-hash). *Proceedings of SECURICOM 1990*, 127–137.

[Mo92] J. H. Moore. Protocol failures in cryptosystems. In *Contemporary Cryptology, The Science of Information Integrity*, pages 541–558. IEEE Press, 1992.

[NBS77] *Data Encryption Standard (DES)*. National Bureau of Standards FIPS Publication 46, 1977.

[NBS80] *DES modes of operation*. National Bureau of Standards FIPS Publication 81, 1980.

[NBS81] *Guidelines for implementing and using the NBS data encryption standard*. National Bureau of Standards FIPS Publication

74, 1981.

[NBS85] *Computer data authentication.* National Bureau of Standards FIPS Publication 113, 1985.

[NBS93] *Secure hash standard.* National Bureau of Standards FIPS Publication 180, 1993.

[NBS94] *Digital signature standard.* National Bureau of Standards FIPS Publication 186, 1994.

[Od87] A. M. Odlyzko (Ed.) *Advances in Cryptology – CRYPTO '86 Proceedings. Lecture Notes in Computer Science*, vol. 263, Springer-Verlag, 1987.

[Ok93] T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. *Lecture Notes in Computer Science*, **740** (1993), 31–53. (Advances in Cryptology – CRYPTO '92.)

[OSS85] H. Ong, C. P. Schnorr and A. Shamir. Efficient signature schemes based on polynomial equations. *Lecture Notes in Computer Science*, **196** (1985), 37–46. (Advances in Cryptology – CRYPTO '84.)

[Pa87] W. Patterson. *Mathematical Cryptology for Computer Scientists and Mathematicians.* Rowman and Littlefield, 1987.

[Pe86] R. Peralta. Simultaneous security of bits in the discrete log. *Lecture Notes in Computer Science*, **219** (1986), 62–72. (Advances in Cryptology – EUROCRYPT '85.)

[Pi86] F. Pichler (Ed.) *Advances in Cryptology – EUROCRYPT '85 Proceedings. Lecture Notes in Computer Science*, vol. 219, Springer-Verlag, 1986.

[PB45] R. L. Plackett and J. P. Burman. The design of optimum multi-factorial experiments. *Biometrika*, **33** (1945), 305–325.

[PH78] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, **24** (1978), 106–110.

[Po88] C. Pomerance (Ed.) *Advances in Cryptology – CRYPTO '87 Proceedings. Lecture Notes in Computer Science*, vol. 293, Springer-Verlag, 1988.

[Po90] C. Pomerance. Factoring. In *Cryptology and Computational Number Theory*, pages 27–47. American Mathematical Society, 1990.

[Po90a] C. Pomerance (Ed.) *Cryptology and Computational Number Theory*, American Mathematical Society, 1990.

[PGV93] B. PRENEEL, R. GOVAERTS AND J. VANDEWALLE. Information authentication: hash functions and digital signatures. *Lecture Notes in Computer Science*, **741** (1993), 87–131. (Computer Security and Industrial Cryptography, State of the Art and Evolution, ESAT Course, May 1991.)

[PGV94] B. PRENEEL, R. GOVAERTS AND J. VANDEWALLE. Hash functions based on block ciphers: a synthetic approach. *Lecture Notes in Computer Science*, **773** (1994), 368–378. (Advances in Cryptology – CRYPTO '93.)

[QG90] J.-J. QUISQUATER AND L. GUILLOU. How to explain zero-knowledge protocols to your children. *Lecture Notes in Computer Science*, **435** (1990), 628–631. (Advances in Cryptology – CRYPTO '89.)

[QV90] J.-J. QUISQUATER AND J. VANDEWALLE (EDS.) *Advances in Cryptology – EUROCRYPT '89 Proceedings. Lecture Notes in Computer Science*, vol. 434, Springer-Verlag, 1990.

[RA79] M. O. RABIN. Digitized signatures and public-key functions as intractible as factorization. *MIT Laboratory for Computer Science Technical Report*, LCS/TR-212, 1979.

[RA80] M. O. RABIN. Probabilistic algorithms for testing primality. *Journal of Number Theory*, **12** (1980), 128–138.

[RI91] R. L. RIVEST. The MD4 message digest algorithm. *Lecture Notes in Computer Science*, **537** (1991), 303–311. (Advances in Cryptology – CRYPTO '90.)

[RSA78] R. L. RIVEST, A. SHAMIR, AND L. ADLEMAN. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, **21** (1978), 120–126.

[RO93] K. H. ROSEN. *Elementary Number Theory and its Applications* (Third Edition). Addison Wesley, 1993.

[RU86] R. A. RUEPPEL. *Analysis and Design of Stream Ciphers*. Springer-Verlag, 1986.

[RU93] R. A. RUEPPEL (ED.) *Advances in Cryptology – EUROCRYPT '92 Proceedings. Lecture Notes in Computer Science*, vol. 658, Springer-Verlag, 1993.

[RV94] R. A. RUEPPEL AND P. C. VAN OORSCHOT Modern key agreement techniques. To appear in *Computer Communications*, 1994.

[SA90] A. SALOMAA. *Public-Key Cryptography*. Springer-Verlag, 1990.

[SC94] J. I. SCHILLER. Secure distributed computing. *Scientific Amer-*

ican, **271**(5) (1994), 72–76.

[Sc93] B. Schneier. *Applied Cryptography, Protocols, Algorithms and Source Code in C*. John Wiley and Sons, 1993.

[Sc91] C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, **4** (1991), 161–174.

[SP89] J. Seberry and J. Pieprzyk *Cryptography: An Introduction to Computer Security*. Prentice-Hall, 1989.

[SP90] J. Seberry and J. Pieprzyk (Eds.) *Advances in Cryptology – AUSCRYPT '90 Proceedings. Lecture Notes in Computer Science*, vol. 453, Springer-Verlag, 1990.

[SZ92] J. Seberry and Y. Zheng (Eds.) *Advances in Cryptology – AUSCRYPT '92 Proceedings. Lecture Notes in Computer Science*, vol. 718, Springer-Verlag, 1993.

[Sh79] A. Shamir. How to share a secret. *Communications of the ACM*, **22** (1979), 612–613.

[Sh84] A. Shamir. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. *IEEE Transactions on Information Theory*, **30** (1984), 699–704.

[Sh90] A. Shamir. An efficient identification scheme based on permuted kernels. *Lecture Notes in Computer Science*, **435** (1990), 606–609. (Advances in Cryptology – CRYPTO '89.)

[Sh94] A. Shamir. Efficient signature schemes based on birational permutations. *Lecture Notes in Computer Science*, **773** (1994), 1–12. (Advances in Cryptology – CRYPTO '93.)

[Sh48] C. E. Shannon. A mathematical theory of communication. *Bell Systems Technical Journal*, **27** (1948), 379–423, 623–656.

[Sh49] C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, **28** (1949), 656–715.

[ST92] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.

[Si85] G. J. Simmons. Authentication theory / coding theory. *Lecture Notes in Computer Science*, **196** (1985), 411–432. (Advances in Cryptology – CRYPTO '84.)

[Si88] G. J. Simmons. A natural taxonomy for digital information authentication schemes. *Lecture Notes in Computer Science*, **293** (1988), 269–288. (Advances in Cryptology – CRYPTO '87.)

[Si92] G. J. Simmons. A survey of information authentication. In *Contemporary Cryptology, The Science of Information In-*

tegrity, pages 379–419. IEEE Press, 1992.

[SI92A] G. J. SIMMONS. An introduction to shared secret and/or shared control schemes and their application. In *Contemporary Cryptology, The Science of Information Integrity*, pages 441–497. IEEE Press, 1992.

[SI92B] G. J. SIMMONS (ED.) *Contemporary Cryptology, The Science of Information Integrity*. IEEE Press, 1992.

[SB92] M. E. SMID AND D. K. BRANSTAD. The data encryption standard: past and future. In *Contemporary Cryptology, The Science of Information Integrity*, pages 43–64. IEEE Press, 1992.

[SB93] M. E. SMID AND D. K. BRANSTAD. Response to comments on the NIST proposed digital signature standard. *Lecture Notes in Computer Science*, **740** (1993), 76–88. (Advances in Cryptology – CRYPTO '92.)

[SS77] R. SOLOVAY AND V. STRASSEN. A fast Monte Carlo test for primality. *SIAM Journal on Computing*, **6** (1977), 84–85.

[ST88] D. R. STINSON. Some constructions and bounds for authentication codes. *Journal of Cryptology*, **1** (1988), 37–51.

[ST90] D. R. STINSON. The combinatorics of authentication and secrecy codes. *Journal of Cryptology*, **2** (1990), 23–49.

[ST92] D. R. STINSON. Combinatorial characterizations of authentication codes. *Designs, Codes and Cryptography*, **2** (1992), 175–187.

[ST92A] D. R. STINSON. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, **2** (1992), 357–390.

[ST94] D. R. STINSON (ED.) *Advances in Cryptology – CRYPTO '93 Proceedings. Lecture Notes in Computer Science*, vol. 773, Springer-Verlag, 1994.

[vHP93] E. VAN HEYST AND T. P. PEDERSEN. How to make efficient fail-stop signatures. *Lecture Notes in Computer Science*, **658** (1993), 366–377. (Advances in Cryptology – EUROCRYPT '92.)

[VV89] S. A. VANSTONE AND P. C. VAN OORSCHOT. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, 1989.

[vT88] H. C. A. VAN TILBORG. *An Introduction to Cryptology*. Kluwer Academic Publishers, 1988.

[vT93] J. VAN TILBURG. Secret-key exchange with authentication. *Lecture Notes in Computer Science*, **741** (1993), 71–86. (Computer Security and Industrial Cryptography, State of the Art and Evolution, ESAT Course, May 1991.)

[VV84] U. VAZIRANI AND V. VAZIRANI. Efficient and secure pseudorandom number generation. In *Proceedings of the 25th Annual Symposium on the Foundations of Computer Science*, pages 458–463. IEEE Press, 1984.

[WA90] M. WALKER. Information-theoretic bounds for authentication systems. *Journal of Cryptology*, **2** (1990), 131–143.

[WE88] D. WELSH. *Codes and Cryptography*. Oxford Science Publications, 1988.

[WI94] M. J. WIENER. Efficient DES key search. Technical report TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994 (also presented at CRYPTO '93 Rump Session).

[WI80] H. C. WILLIAMS. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, **26** (1980), 726–729.

[WI86] H. C. WILLIAMS (ED.) *Advances in Cryptology – CRYPTO '85 Proceedings. Lecture Notes in Computer Science*, vol. 218, Springer-Verlag, 1986.

[YA82] A. YAO. Theory and applications of trapdoor functions. In *Proceedings of the 23rd Annual Symposium on the Foundations of Computer Science*, pages 80–91. IEEE Press, 1982.

Index

Previous Chapter Previous Page Home Next page

Previous Chapter Previous Page Home Next page

Previous Chapter Previous Page Home Next page

Previous Chapter Previous Page Home Next page

Previous Chapter Previous Page Home Next page

Previous Chapter Previous Page Home Next page