References

[Adl] L. Adleman: On breaking the iterated Merkle-Hellman public key cryptosystem. Proceedings 15th ACM Symposium on the Theory of Computing, 1983, pp. 402–412

[Ang] D. Angluin: Lecture Notes on the Complexity of Some Problems in Number Theory. Yale University, Computer Science Department, Technical Report 243, 1982

[BeP] H. Beker and F. Piper: Cipher systems. Northwood Books, London 1982

[BeG] M. Bellare and S. Goldwasser: New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs. CRYPTO-89 Abstracts, University of California, Santa Barbara 1989, pp. 189–204

[Ben] J.D.C. Benaloh: Verifiable secret-ballot elections. Yale University, Computer Science Department, Technical Report 561, 1987

[BenT] J.D.C. Benaloh and D. Tuinstra: Receipt-free secret-ballot elections. Proceedings STOC-94, (1994) 544–553

[Bl1] M. Blum: Coin flipping by telephone. A protocol for solving impossible problems. SIGACT News, 1981, pp. 23–27

[Bl2] M. Blum: How to prove a theorem so no one else can claim it. Proceedings International Congress of Mathematicians, 1987, pp. 1444–1451

[Bo] B. den Boer: More efficient match-making and satisfiability; the five card trick. Proceedings EUROCRYPT-89, Lecture Notes in Computer Science, vol. 434. Springer, Berlin 1990, pp. 208–217

[BC] R.C. Bose and S. Chowla: Theorems in the additive theory of numbers. Comment. Math. Helvet. 37 (1962) 141–147

[Br1] G. Brassard: A note on the complexity of cryptography. IEEE Transactions on Information Theory IT-25 (1979) 232–233

[Br2] G. Brassard: Modern cryptology. Lecture Notes in Computer Science, vol. 325. Springer, Berlin 1988

[BCC] G. Brassard, D. Chaum and C. Crépeau: An introduction to minimum disclosure. Amsterdam CWI Quarterly l (1988) 3–17

[BCR] G. Brassard, C. Crépeau and J.-M. Robert: All-or-nothing disclosure of secrets. Lecture Notes in Computer Science, vol. 263. Springer, Berlin 1987, pp. 234–238

[BuP] H. Burk and A. Pfitzmann: Digital payment systems enabling security and unobservability. Computers and Security 9 (1989) 399–416

[Cho] B.-Z. Chor: Two issues in public key cryptography. MIT Press, Cambridge, Mass. 1986

[Cop] D. Coppersmith: Fast evaluation of logarithms in fields of characteristic two. IEEE Transactions on Information Theory IT-30 (1984) 587–594

[CrK] C. Crépeau and J. Kilian: Discreet solitary games. Proceedings CRYPTO-93, Lecture Notes in Computer Science, vol. 773. Springer, Berlin 1994, pp. 319–330

[Dam] I.B. Damgaard: On the existence of bit commitment schemes and zero-knowledge proofs. CRYPTO-89 Abstracts, University of California, Santa Barbara 1989, pp. 15–23

[Del] J.M. Delaurentis: A further weakness in the common modulus protocol for the RSA cryptoalgorithm. Cryptologia 8 (1984) 253–259

[De] D.E. Denning: Cryptography and data security. Addison-Wesley, Reading, Mass. 1982

[DMP] A. De Santis, S. Micali and G. Persiano: Non-interactive zero-knowledge proof systems. Lecture Notes in Computer Science, vol. 293. Springer, Berlin 1987, pp. 52–72

[DGB] Y. Desmedt, C. Goutier and S. Bengio: Special uses and abuses of the Fiat-Shamir passport protocol. Lecture Notes in Computer Science, vol. 293. Springer, Berlin 1987, pp. 21–39

[DH] W. Diffie and M. Hellman: New directions in cryptography. IEEE Transactions on Information Theory IT-22 (1976) 644–654

[EIG] T. El Gamal: A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory IT-31 (1985) 469–473

[EvY] S. Even and Y. Yacobi: Cryptosystems which are *NP*-hard to break. Technion, Computer Science Department, Technical Report 1979

[FFS] U. Feige, A. Fiat and A. Shamir: Zero knowledge proofs of identity. Journal of Cryptology 1 (1988) 77–94

[FiS] A. Fiat and A. Shamir: How to prove yourself: practical solutions to identification and signature problems. Lecture Notes in Computer Science, vol. 263. Springer, Berlin 1987, pp. 186–194

[Fl] D. Floyd: Annotated bibliography in conventional and public key cryptography. Cryptologia 7 (1983) 12–24

[Ga] H.F. Gaines. Cryptoanalysis. Dover Publications, New York 1939

[GMW] O. Goldreich, S. Micali and A. Widgerson: How to prove all *NP*-statements in zero-knowledge, and a methodology of cryptographic protocol design. Lecture Notes in Computer Science, vol. 263. Springer, Berlin 1987, pp. 171–185

[GM] S. Goldwasser and S. Micali; Probabilistic encryption. Journal of Computer and Systems Sciences 28 (1984) 270–299

[GMR] S. Goldwasser, S. Micali and C. Rackoff: The knowledge complexity of interactive proof systems. Proceedings 17th ACM Symposium on the Theory of Computing, 1985, pp. 291–304

[GMT] S. Goldwasser, S. Micali and P. Tong: Why and how to establish a private code on a public network. Proceedings 23rd FOCS Symposium, 1982, pp. 134–144

[Hil] L.S. Hill: Cryptography in an algebraic alphabet. American Mathematical Monthly 36 (1929) 306–312

[Ka] D. Kahn: The codebreakers: the story of secret writing. Macmillan, New York 1967

[Kar1] J. Kari: A cryptosystem based on propositional logic. Lecture Notes in Computer Science, vol. 381. Springer, Berlin 1989, pp. 210–219

[Kar2] J. Kari: A cryptanalytic observation concerning systems based on language theory. Discrete Applied Mathematics 21 (1988) 265–268

[Kar3] J. Kari: Observations concerning a public-key cryptosystem based on iterated morphisms. Theoretical Computer Science 66 (1989) 45–53

[Ko] N. Koblitz: A course in number theory and cryptography. Springer, Berlin 1987

[Kon] A. Konheim: Cryptography: a primer. Wiley and Sons, New York 1982

[Kra] E. Kranakis: Primality and cryptography. Wiley-Teubner, Chichester New York Stuttgart 1986

[McE] R.J. McEliece: A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report. Jet Propulsion Labs, Pasadena 42–44 (1978) 114–116

[MeH] R. Merkle and M. Hellman: Hiding information and signatures in trapdoor knapsacks. IEEE Transactions on Information Theory IT-24 (1978) 525–530

[Mig] M. Mignotte: How to share a secret. Lecture Notes in Computer Science, vol. 149. Springer, Berlin 1983, pp. 371–375

[Mil] G.L. Miller: Riemann's hypothesis and tests for primality. Journal of Computer and System Sciences 13 (1976) 300–317

[Nie] V. Niemi: Hiding regular languages: a public-key cryptosystem. Manuscript 1989

[NieR] V. Niemi and A. Renvall: Efficient voting with no selling of votes. Manuscript 1995, submitted for publication

[NieR2] V. Niemi and A. Renvall: Secure multiparty computations without computers. Theoretical Computer Science, to appear

[NuS] H. Nurmi and A. Salomaa: On the cryptography of secret ballot. Behavioral Science 36 (1991) 34–40

[NuSS] H. Nurmi, A. Salomaa and L. Santean: Secret-ballot elections in computer networks. Computers and Security 10 (1991) 553–560

[Odl] A.M. Odlyzko: Discrete logarithms in finite fields and their cryptographic significance. Lecture Notes in Computer Science, vol. 209. Springer, Berlin 1985, pp. 224–314

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

[PIK] C. Park, K. Itoh and K. Kurosawa: Efficient anonymous channel and all/nothing election scheme. Proceedings EUROCRYPT-93, Lecture Notes in Computer Science, vol. 765. Springer, Berlin 1994. pp. 248–259

[Rab1] M.O. Rabin: Digitalized signatures and public key functions as intractable as factorization. MIT, Laboratory for Computer Science, Technical Report 212, 1979

[Rab2] M.O. Rabin: How to exchange secrets by oblivious transfer. Aiken Computation Laboratory, Harvard University, Technical Report TR-*81*, 1981

[Ren] Tao Renji: Some results on the structure of feedforward inverses. Scientia Sinica, Ser. A 27 (1984) 157–162

[Renv] A. Renvall: Cryptographic protocols and techniques for communication. Dissertation, Univ. of Turku 1994

[RSA] M. Rivest, A. Shamir and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21 (1978) 120–126

[RS] G. Rozenberg and A. Salomaa: The mathematical theory of *L* systems. Academic Press, New York 1980

[Sa1] A. Salomaa: Computation and automata. Cambridge University Press, Cambridge 1985. Available also in French and Japanese

[Sa2] A. Salomaa: A public-key cryptosystem based on language theory. Computers and Security 7 (1988) 83–87

[Sa3] A. Salomaa: A deterministic algorithm for modular knapsack problems. Theoretical Computer Science 88 (1991) 127–138

[Sa4] A. Salomaa: Decision problems arising from knapsack transformations. Acta Cybernetica 9 (1990) 419–440

[SaY] A. Salomaa and S. Yu: On a public-key cryptosystem based on iterated morphisms and substitutions. Theoretical Computer Science 48 (1986) 283–296

[SchA] C.P. Schnorr and W. Alexi: RSA-bits are $0.5 + \varepsilon$ secure. Lecture Notes in Computer Science, vol. 209. Springer, Berlin 1985, pp. 113–126

[Schn] B. Schneier: Applied Cryptography. John Wiley, New York 1993, 2nd ed. 1995

[SP] J. Seberry and J. Pieprzyk: Cryptography: an introduction to computer security. Prentice Hall, New York 1989

[Sh1] A. Shamir: A fast signature scheme. MIT, Laboratory for Computer Science, Technical Report 1978

[Sh2] A. Shamir: A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. Proceedings 23rd FOCS Symposium, 1982, pp. 145–152

[Sh3] A. Shamir: Embedding cryptographic trapdoors in arbitrary knapsack systems. MIT, Laboratory for Computer Science, Technical Report 230, 1982

[Sh4] A. Shamir: Identity based cryptosystems and signature schemes. Lecture Notes in Computer Science, vol. 196. Springer, Berlin 1985, pp. 47–53

[Sh5] A. Shamir: An efficient identification scheme based on permuted kernels. Weizmann Institute, Department of Applied Mathematics, Technical Report 1989

[ShRA] A. Shamir, R. Rivest and L. Adleman: Mental poker. In D.A. Klarner (ed.), The mathematical gardener. Wadsworth International, Belmont 1981, pp. 37–43

[Shan] C.E. Shannon: Communication theory of secrecy systems. Bell System Technical Journal 28 (1949) 656–715

[SiS] R. Siromoney and G. Siromoney: A public key cryptosystem that defies cryptanalysis. EATCS Bulletin 28 (1986) 37–43

[Til] H.C.A. Van Tilborg: An introduction to cryptology. Kluwer Academic Publishers, Boston 1988

[WaM] N.R. Wagner and M.R. Magyarik: A public key cryptosystem based on the word problem. Lecture Notes in Computer Science, vol. 196. Springer, Berlin 1985, pp. 19–37

[Wel] D. Welsh: Codes and cryptography. Oxford University Press, Oxford 1988

[Wie] M.J. Wiener: Cryptanalysis of short RSA secret exponents. Proceedings EUROCRYPT-89. Lecture Notes in Computer Science, vol. 434. Springer, Berlin 1990, p. 372. Full paper: IEEE Transactions on Information Theory IT-36 (1990) 553–558

[Wil] H.C. Williams: Some public-key crypto-functions as intractable as factorization. Cryptologia 9 (1985) 223–237

[Yao] A.C. Yao: Protocols for secure computations. Proceedings 23rd FOCS Symposium, 1982, pp. 160–164

[Zim] H.S. Zim: Codes and secret writing. Scholastic Book Services, New York 1948