References

Textbooks

[Ash65] R.B. Ash: Information Theory. New York: John Wiley & Sons, 1965.

[BalDiaGab95] J.L. Balcázar, J. Díaz, J. Gabarró: Structural Complexity I. Berlin, Heidelberg, New York: Springer-Verlag, 1995.

[Bauer96] H. Bauer: Probability Theory. Berlin: de Gruyter, 1996.

[BerPer85] J. Berstel, D. Perrin: Theory of Codes. Orlando: Academic Press, 1985.

[Buchmann2000] J.A. Buchmann: Introduction to Cryptography. Berlin, Heidelberg, New York: Springer-Verlag, 2000.

[Cohen95] H. Cohen: A Course in Computational Algebraic Number Theory. Berlin, Heidelberg, New York: Springer-Verlag, 1995.

[CovTho92] T.M. Cover, J.A. Thomas: Elements of Information Theory. New York: John Wiley & Sons, 1992.

[Feller68] W. Feller: An Introduction to Probability Theory and its Applications. 3rd ed. New York: John Wiley & Sons, 1968.

[Forster96] O. Forster: Algorithmische Zahlentheorie. Braunschweig, Wiesbaden: Vieweg, 1996.

[GanYlv67] R.A. Gangolli, D. Ylvisaker: Discrete Probability. New York: Harcourt, Brace & World, 1967.

[Goldreich99] O. Goldreich: Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Berlin, Heidelberg, New York: Springer-Verlag, 1999.

[Goldreich01] O. Goldreich: Foundations of Cryptography - Basic Tools. Cambridge University Press, 2001.

[GolPeiSch94] S.W. Golomb, R.E. Peile, R.A. Scholtz: Basic Concepts in Information Theory and Coding. New York: Plenum Press, 1994.

[Gordon97] H. Gordon: Discrete Probability. Berlin, Heidelberg, New York: Springer-Verlag, 1997.

[Hamming86] R.W. Hamming: Coding and Information Theory. 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1986.

[HarWri79] G.H. Hardy, E.M. Wright: An Introduction to the Theory of Numbers. 5th ed. Oxford: Oxford University Press, 1979.

[HopUll79] J. Hopcroft, J. Ullman: Introduction to Automata Theory, Languages and Computation. Reading, MA: Addison-Wesley Publishing Company, 1979.

[IreRos82] K. Ireland, M.I. Rosen: A Classical Introduction to Modern Number Theory. Berlin, Heidelberg, New York: Springer-Verlag, 1982.

[Kahn67] D. Kahn: The Codebreakers: The Story of Secret Writing. New York: Macmillan Publishing Co. 1967.

[Knuth98] D.E. Knuth: The Art of Computer Programming. 3rd ed. Volume 2 / Seminumerical Algorithms. Reading, MA: Addison-Wesley Publishing Company, 1998.

[Koblitz94] N. Koblitz: A Course in Number Theory and Cryptography. 2nd ed. Berlin, Heidelberg, New York: Springer-Verlag, 1994.
[Luby96] M. Luby: Pseudorandomness and Cryptographic Applications. Princeton, NJ: Princeton University Press, 1996.
[MenOorVan96] A. Menezes, P.C. van Oorschot, S.A. Vanstone: Handbook of Applied Cryptography. Boca Raton, New York, London, Tokyo: CRC-Press, 1996.
[MotRag95] R. Motwani, P. Raghavan: Randomized Algorithms. Cambridge, UK: Cambridge University Press, 1995.
[Osen74] L.M. Osen: Women in Mathematics. Cambridge, MA: MIT, 1974.
[Papadimitriou94] C.H. Papadimitriou: Computational Complexity. Reading, MA: Addison-Wesley Publishing Company, 1994.
[Rényi70] A. Rényi: Probability Theory. Amsterdam: North-Holland, 1970.
[Riesel94] H. Riesel: Prime Numbers and Computer Methods for Factorization. Boston, Basel: Birkhäuser, 1994.
[Rose94] H.E. Rose: A Course in Number Theory. 2nd ed. Oxford: Clarendon Press, 1994.
[Rosen2000] K.H. Rosen: Elementary Number Theory and its Applications. 4th ed. Reading, MA: Addison-Wesley Publishing Company, 2000.
[Salomaa90] A. Salomaa: Public-Key Cryptography. Berlin, Heidelberg, New York: Springer-Verlag, 1990.
[Schneier96] B. Schneier: Applied Cryptography. New York: John Wiley & Sons, 1996.
[Simmons92] G.J. Simmons (ed.): Contemporary Cryptology. Piscataway, NJ: IEEE-Press, 1992.
[Stinson95] D.R. Stinson: Cryptography - Theory and Practice. Boca Raton, New York, London, Tokyo: CRC-Press, 1995.

Papers

[AleChoGolSch88] W.B. Alexi, B. Chor, O. Goldreich, C.P. Schnorr: RSA/Rabin functions: certain parts are as hard as the whole. SIAM Journal on Computing, 17(2): 194–209, April 1988.
[AumDinRab02] Y. Aumann, Y.Z. Ding, M.O. Rabin: Everlasting security in the bounded storage model. To appear in IEEE Transactions on Information Theory, April, 2002.
[AumRab99] Y. Aumann, M.O. Rabin: Information-theoretically secure communication in the limited storage space model. Advances in Cryptology - CRYPTO '99, Lecture Notes in Computer Science, 1666: 65–79, Springer-Verlag, 1999.
[Bach88] E. Bach: How to generate factored random numbers. SIAM Journal on Computing, 17(2): 179–193, April 1988.
[BarPfi97] N. Barić, B. Pfitzmann: Collision-free accumulators and fail-stop signature schemes without trees. Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Science, 1233: 480–494, Springer-Verlag, 1997.
[BatHor62] P. Bateman, R. Horn: A heuristic formula concerning the distribution of prime numbers. Mathematics of Computation, 16: 363–367, 1962.
[BatHor65] P. Bateman, R. Horn: Primes represented by irreducible polynomials in one variable. Proc. Symp. Pure Math., 8: 119–135, 1965.
[BeGrGwHåKiMiRo88] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali, P. Rogaway: Everything provable, is provable in zero-knowledge. Advances in Cryptology - CRYPTO '88, Lecture Notes in Computer Science, 403: 37–56, Springer-Verlag, 1990.
[Bellare99] M. Bellare : Practice oriented provable security. Lectures on Data Security. Lecture Notes in Computer Science, 1561: 1–15, Springer-Verlag, 1999.

[BelRog94] M. Bellare, P. Rogaway: Optimal asymmetric encryption. Advances in Cryptology - EUROCRYPT '94, Lecture Notes in Computer Science, 950: 92–111, Springer-Verlag, 1995.

[BelRog96] M. Bellare, P. Rogaway: The exact security of digital signatures, how to sign with RSA and Rabin. Advances in Cryptology - EUROCRYPT '96, Lecture Notes in Computer Science, 1070: 399–416, Springer-Verlag, 1996.

[BelRog97] M. Bellare, P. Rogaway: Collision-resistant hashing: towards making UOWHF practical. Advances in Cryptology - CRYPTO '97, Lecture Notes in Computer Science, 1294: 470–484, Springer-Verlag, 1997.

[Bleichenbacher96] D. Bleichenbacher: Generating ElGamal signatures without knowing the secret key. Advances in Cryptology - EUROCRYPT '96, Lecture Notes in Computer Science, 1070: 10–18, Springer-Verlag, 1996.

[BluBluShu86] L. Blum, M. Blum, M. Shub: A simple unpredictable pseudorandom number generator. SIAM Journal on Computing, 15(2): 364–383, 1986.

[BluGol85] M. Blum, S. Goldwasser: An efficient probabilistic public-key encryption scheme which hides all partial information. Advances in Cryptology - Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 196: 289–299, Springer-Verlag, 1985.

[Blum82] M. Blum: Coin flipping by telephone: a protocol for solving impossible problems. Proceedings of the 24th IEEE Computer Conference, San Francisco, Calif., February 22–25, 1982: 133-137, 1982.

[Blum83] M. Blum: Independent unbiased coin flips from a correlated biased source. Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, Singer Islands, Fla., October 24–26, 1984: 425–433, 1984.

[BluMic84] M. Blum, S. Micali: How to generate cryptographically strong sequences of pseudorandom bits. SIAM Journal on Computing, 13(4): 850–863, November 1984.

[Boer88] B. Den Boer: Diffie-Hellman is as strong as discrete log for certain primes. Advances in Cryptology - CRYPTO '88, Lecture Notes in Computer Science, 403: 530–539, Springer-Verlag, 1990.

[BonVen96] D. Boneh, R. Venkatesan: Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes. Advances in Cryptology - CRYPTO '96, Lecture Notes in Computer Science, 1109: 129–142, Springer-Verlag, 1996.

[Brands93] S. Brands: An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323. Amsterdam, NL: Centrum voor Wiskunde en Informatica (CWI), 1993.

[BraCre96] G. Brassard, C. Crepeau: 25 years of quantum cryptography. SIGACT News 27(3): 13–24, 1996.

[CachMau97] C. Cachin, U.M. Maurer: Unconditional security against memory-bounded adversaries. Advances in Cryptology - CRYPTO '96, Lecture Notes in Computer Science, 1109: 292–306, Springer-Verlag, 1996.

[CamMauSta96] J. Camenisch, U.M. Maurer, M. Stadler: Digital payment systems with passive anonymity revoking trustees. Proceedings of ESORICS '96, Lecture Notes in Computer Science, 1146: 33-43, Springer-Verlag, 1996.

[CamWie92] K. W. Campbell, M. J. Wiener: DES is not a group. Advances in Cryptology - CRYPTO '92, Lecture Notes in Computer Science, 740: 512–520, Springer-Verlag, 1993.

[CamPivSta94] J.L. Camenisch, J.M. Piveteau, M.A. Stadler: Blind signatures based on the discrete logarithm problem. Advances in Cryptology - EUROCRYPT '94, Lecture Notes in Computer Science, 950: 428–432, Springer-Verlag, 1995.

[CanGolHal98] R. Canetti, O. Goldreich, S. Halevi: The random oracle methodology, revisited. STOC'98, Dallas, Texas: 209–218, New York, NY: ACM, 1998.

[CarWeg79] J.L. Carter, M.N. Wegman: Universal classes of hash functions. Journal of Computer and System Sciences, 18: 143–154, 1979.

[ChaPed92] D. Chaum, T. Pedersen: Wallet databases with observers. Advances in Cryptology - CRYPTO '92, Lecture Notes in Computer Science, 740: 89–105, Springer-Verlag, 1993.

[Chaum82] D. Chaum: Blind signatures for untraceable payments. Advances in Cryptology - Proceedings of CRYPTO 82: 199–203, Plenum Press 1983.

[CraDam96] R. Cramer, I. Damgård: New generation of secure and practical RSA-based signatures. Advances in Cryptology - CRYPTO '96, Lecture Notes in Computer Science, 1109: 173–185, Springer-Verlag, 1996.

[CraFraSchYun96] R. Cramer, M.K. Franklin, B. Schoenmakers, M. Yung: Multi-authority secret-ballot elections with linear work. Advances in Cryptology - EUROCRYPT '96, Lecture Notes in Computer Science, 1070: 72–83, Springer-Verlag, 1996.

[CraGenSch97] R. Cramer, R. Gennaro, B. Schoenmakers: A secure and optimally efficient multi-authority election scheme. Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Science, 1233: 103–118, Springer-Verlag, 1997.

[CraSho2000] R. Cramer, V. Shoup: Signature schemes based on the strong RSA assumption. ACM Transactions on Information and System Security, 3(3): 161–185, 2000.

[Damgård87] I.B. Damgård: Collision-free hash functions and public-key signature schemes. Advances in Cryptology - EUROCRYPT '87, Lecture Notes in Computer Science, 304: 203-216, Springer-Verlag, 1988.

[Diffie88] W. Diffie: The first ten years of public key cryptology. In: G.J. Simmons (ed.): Contemporary Cryptology, 135–175, Piscataway, NJ: IEEE-Press, 1992.

[DifHel76] W. Diffie, M.E. Hellman: New directions in cryptography. IEEE Transactions on Information Theory, IT-22: 644–654, 1976.

[DifHel77] W. Diffie, M. E. Hellman: Exhaustive cryptanalysis of the NBS data encryption standard. Computer, 10: 74–84, 1977.

[Ding01] Y.Z. Ding: Provable everlasting security in the bounded storage model. PhD Thesis, Cambridge, MA: Harvard University, May 2001.

[DinRab01] Y.Z. Ding, M.O. Rabin: Hyper-encryption and everlasting security. Preprint, October 10, 2001.

[Dobbertin96] H. Dobbertin: Welche Hash-Funktionen sind für digitale Signaturen geeignet? In: P. Horster (ed.): Digitale Signaturen, 81–92, Braunschweig, Wiesbaden: Vieweg 1996.

[DwoNao94] C. Dwork, M. Naor: An efficient unforgeable signature scheme and its applications. Advances in Cryptology - CRYPTO '94, Lecture Notes in Computer Science, 839: 234–246, Springer-Verlag, 1994.

[ElGamal84] T. ElGamal: A public key cryptosystem and a signature scheme based on discrete logarithms. Advances in Cryptology - Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 196: 10–18, Springer-Verlag, 1985.

[FiaSha86] A. Fiat, A. Shamir: How to prove yourself: practical solutions to identification and signature problems. Advances in Cryptology - CRYPTO '86, Lecture Notes in Computer Science, 263: 186–194, Springer-Verlag, 1987.

[FIPS46 1977] FIPS46: 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.

[FisSch2000] R. Fischlin, C.P. Schnorr: Stronger security proofs for RSA and Rabin bits. Journal of Cryptology, 13(2): 221–244, 2000.

[FujOkaPoiSte2001] E. Fujisaki, T. Okamoto, D. Pointcheval, J. Stern: RSA-OAEP is secure under the RSA assumption. Advances in Cryptology - CRYPTO '2001, Lecture Notes in Computer Science, 2139: 260–274, Springer-Verlag, 2001.

[GenHalRab99] R. Gennaro, S. Halevi, T. Rabin: Secure hash-and-sign signatures without the random oracle. Advances in Cryptology - EUROCRYPT '99, Lecture Notes in Computer Science, 1592: 123–139, Springer-Verlag, 1999.

[GenJarKraRab99] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin: Secure distributed key generation for discrete-log based cryptosystems. Advances in Cryptology - EUROCRYPT '99, Lecture Notes in Computer Science, 1592: 295–310, Springer-Verlag, 1999.

[Gill77] J. Gill: Computational complexity of probabilistic Turing machines. SIAM Journal on Computing, 6(4): 675–695, December 1977.

[GolLev89] O. Goldreich, L. Levin: A hard-core predicate for all one-way functions. Proceedings of the 21st Annual ACM Symposium on Theory of Computing, Seattle, Wash., May 15–17, 1989: 25–32, 1989.

[GolMic84] S. Goldwasser, S. Micali: Probabilistic encryption. Journal of Computer and System Sciences, 28(2): 270–299, 1984.

[GolMicRac89] S. Goldwasser, S. Micali, C. Rackoff: The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 18: 185–208, 1989.

[GolMicRiv88] S. Goldwasser, S. Micali, R. Rivest: A digital signature scheme secure against chosen message attacks. SIAM Journal on Computing, 17(2): 281–308, 1988.

[GolMicTon82] S. Goldwasser, S. Micali, P. Tong: Why and how to establish a private code on a public network. Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science, Chicago, Ill., November 3–5, 1982: 134–144, 1982.

[GolMicWid86] O. Goldreich, S. Micali, 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, Toronto, October 27–29, 1986: 174–187, 1986.

[Gordon84] J.A. Gordon: Strong primes are easy to find. Advances in Cryptology - EUROCRYPT '84, Lecture Notes in Computer Science, 209: 216-223, Springer-Verlag, 1985.

[ISO/IEC 9594-8] Information technology - Open Systems Interconnection - The Directory: Authentication framework. International Organization for Standardization, Geneva, Switzerland, 1995.

[ISO/IEC 10116] Information processing - Modes of operation for an n-bit block cipher algorithm. International Organization for Standardization, Geneva, Switzerland, 1991.

[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.

[Koblitz88] N. Koblitz: Primality of the number of points on an elliptic curve over a finite field. Pacific Journal of Mathematics, 131(1): 157-165, 1988.

[LeeMooShaSha55] K. de Leeuw, E.F. Moore, C.E. Shannon, N. Shapirio: Computability by probabilistic machines. In: C.E. Shannon, J. McCarthy (eds.): Automata Studies, 183 -212, Princeton, NJ: Princeton University Press, 1955.

[MatMeyOse85] S.M. Matyas, C.H. Meyer, J. Oseas: Generating strong one way functions with cryptographic algorithm. IBM Techn. Disclosure Bull., 27(10A), 1985.

[MatTakIma86] T. Matsumoto, Y. Takashima, H. Imai: On seeking smart public-key-distribution systems. The Transactions of the IECE of Japan, E69: 99–106, 1986.

[Maurer92] U.M. Maurer: Conditionally-perfect secrecy and a provably-secure randomized cipher. Journal of Cryptology, 5(1): 53–66, 1992.

[Maurer94] U.M. Maurer: Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms. Advances in Cryptology - CRYPTO '94, Lecture Notes in Computer Science, 839: 271–281, Springer-Verlag, 1994.

[Maurer95] U.M. Maurer: Fast generation of prime numbers and secure public-key cryptographic parameters. Journal of Cryptology, 8: 123–155, 1995.

[Maurer97] U.M. Maurer: Information-theoretically secure secret-key agreement by not authenticated public discussion. Advances in Cryptology - EUROCRYPT '92, Lecture Notes in Computer Science, 658: 209–225, Springer-Verlag, 1993.

[Maurer99] U.M. Maurer: Information-theoretic cryptography. Advances in Cryptology - CRYPTO '99, Lecture Notes in Computer Science, 1666: 47–65, Springer-Verlag, 1999.

[MauWol96] U.M. Maurer, S. Wolf: Diffie-Hellman oracles. Advances in Cryptology - CRYPTO '96, Lecture Notes in Computer Science, 1109: 268–282, Springer-Verlag, 1996.

[MauWol97] U.M. Maurer, S. Wolf: Privacy amplification secure against active adversaries. Advances in Cryptology - CRYPTO '96, Lecture Notes in Computer Science, 1109: 307–321, Springer-Verlag, 1996.

[MauWol98] U.M. Maurer, S. Wolf: Diffie-Hellman, Decision Diffie-Hellman, and discrete logarithms. Proceedings of ISIT '98, Cambridge, MA, August 16–21, 1998, IEEE Information Theory Society: 327, 1998.

[MauWol2000] U.M. Maurer, S. Wolf: The Diffie-Hellman protocol. Designs, Codes, and Cryptography, Special Issue Public Key Cryptography, 19: 147–171, Kluwer Academic Publishers, 2000.

[MicRacSlo88] S. Micali, C. Rackoff, B. Sloan: The notion of security for probabilistic cryptosystems. SIAM Journal on Computing, 17: 412–426, 1988.

[NaoYun89] M. Naor, M. Yung: Universal one-way hash functions and their cryptographic applications. Proceedings of the 21st Annual ACM Symposium on Theory of Computing, Seattle, Wash., May 15–17, 1989: 33–43, 1989.

[NeeSch78] R.M. Needham, M.D. Schroeder: Using encryption for authentication in large networks of computers. Communications of the ACM, 21: 993–999, 1978.

[von Neumann63] J. von Neumann: Various techniques for use in connection with random digits. In: von Neumann's Collected Works, 768–770. New York: Pergamon, 1963.

[NeuTs'o94] B.C. Neuman, T. Ts'o: Kerberos: an authentication service for computer networks. IEEE Communications Magazine, 32: 33–38, 1994.

[Newman80] D.J. Newman: Simple analytic proof of the prime number theorem. Am. Math. Monthly 87: 693–696, 1980.

[NIST94] National Institute of Standards and Technology, NIST FIPS PUB 186, Digital Signature Standard, U.S. Department of Commerce, 1994.

[Okamoto92] T. Okamoto: Provably secure and practical identification schemes and corresponding signature schemes. Advances in Cryptology - CRYPTO '92, Lecture Notes in Computer Science, 740: 31–53, Springer-Verlag, 1993.

[OkaOht91] T. Okamoto, K. Ohta: Universal electronic cash. Advances in Cryptology - CRYPTO '91, Lecture Notes in Computer Science, 576: 324–337, Springer-Verlag, 1992.

[OngSchSha84] H. Ong, C.P. Schnorr, A. Shamir: Efficient signature schemes based on quadratic equations. Advances in Cryptology - Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 196: 37–46, Springer-Verlag, 1985.

[Pedersen91] T. Pedersen: A threshold cryptosystem without a trusted party. Advances in Cryptology - EUROCRYPT '91, Lecture Notes in Computer Science, 547: 522–526, Springer-Verlag, 1991.

[Peralta92] R. Peralta: On the distribution of quadratic residues and nonresidues modulo a prime number. Mathematics of Computation, 58(197): 433–440, 1992.

[Pfitzmann96] B. Pfitzmann: Digital signature schemes - general framework and fail-stop signatures. Lecture Notes in Computer Science, 1100, Springer-Verlag, 1996.

[PohHel78] S.C. Pohlig, M.E. Hellman: An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Transactions on Information Theory, IT24: 106–110, January 1978.

[PoiSte2000] D. Pointcheval, J. Stern: Security arguments for digital signatures and blind signatures. Journal of Cryptology, 13(3): 361-396, 2000.

[PolSch87] J.M. Pollard, C.P. Schnorr: An efficient solution of the congruence $x^2 + ky^2 = m(\mathrm{mod} n)$. IEEE Transactions on Information Theory, 33(5): 702–709, 1987.

[Rabin63] M.O. Rabin: Probabilistic automata. Information and Control, 6: 230-245, 1963.

[Rabin79] M. O. Rabin: Digitalized signatures and public key functions as intractable as factorization. MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[Rényi61] A. Rényi: On measures of entropy and information. Proc. 4th Berkeley Symposium on Mathematical Statistics and Probability, vol. 1: 547–561, Berkeley: Univ. of Calif. Press, 1961.

[RFC 1510] RFC 1510: The Kerberos network authentication service (V5). Internet Request for Comments 1510, J. Kohl, C. Neuman, 1993.

[Rivest90] R. Rivest: The MD4 message digest algorithm. Advances in Cryptology - CRYPTO '90, Lecture Notes in Computer Science, 537: 303–311, Springer-Verlag, 1991.

[RivShaAdl78] R. Rivest, A. Shamir, and L.M. Adleman: A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2): 120–126, 1978.

[RosSch62] J. Rosser, L. Schoenfield: Approximate formulas for some functions of prime numbers. Illinois J. Math. 6: 64–94, 1962.

[Santos69] E.S. Santos: Probabilistic Turing machines and computability. Proc. Amer. Math. Soc. 22: 704–710, 1969.

[SchnAle84] C.P. Schnorr, W. Alexi: RSA-bits are 0.5 + epsilon secure. Advances in Cryptology - EUROCRYPT '84, Lecture Notes in Computer Science, 209: 113–126, Springer-Verlag, 1985.

[Shannon48] C.E. Shannon: A mathematical theory of communication. Bell Systems Journal, 27: 379–423, 623–656, 1948.

[Shannon49] C.E. Shannon: Communication theory of secrecy systems. Bell Systems Journal, 28: 656–715, 1949.

[Shor94] P.W. Shor: Algorithms for quantum computation: discrete log and factoring. Proceedings of the IEEE 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, November 20–22, 1994: 124–134, 1994.

[Shoup2001] V. Shoup: OAEP Reconsidered. Advances in Cryptology - CRYPTO '2001, Lecture Notes in Computer Science, 2139: 239–259, Springer-Verlag, 2001.

[Stinson92] D.R. Stinson: Universal hashing and authentication codes. Advances in Cryptology - CRYPTO '91, Lecture Notes in Computer Science, 576: 74–85, Springer-Verlag, 1992.

[Vazirani85] U.V. Vazirani: Towards a strong communication complexity, or generating quasi-random sequences from slightly random sources. Proceedings of the 17th Annual ACM Symposium on Theory of Computing, Providence, RI, May 6–8, 1985: 366–378, 1985.

[VazVaz84] U.V. Vazirani, V.V. Vazirani: Efficient and secure pseudorandom number generation. Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, Singer Islands, Fla., October 24–26, 1984: 458–463, 1984.

[Vernam19] G.S. Vernam: Secret signaling system. U.S. Patent # 1, 310, 719, 1919.

[Vernam26] G.S. Vernam: Cipher printing telegraph systems for secret wire and radio telegraphic communications. Journal of of American Institute for Electrical Engineers, 45: 109-115, 1926.

[WaiPfi89] M. Waidner, B. Pfitzmann: The dining cryptographers in the disco: unconditional sender and recipient untraceability with computationally secure serviceability. Advances in Cryptology - EUROCRYPT '89, Lecture Notes in Computer Science, 434: 690, Springer-Verlag, 1990.

[WegCar81] M.N. Wegman, J.L. Carter: New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences, 22: 265–279, 1981.

[Wiener90] M.J. Wiener: Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, 36: 553–558, 1990.

[Wolf98] S. Wolf: Unconditional security in cryptography. In: I. Damgård (ed.): Lectures on Data Security. Lecture Notes in Computer Science, 1561: 217–250, Springer-Verlag, 1998.

Internet

[BelDesJokRog97] M. Bellare, A. Desai, E. Jopkipii, P. Rogaway: A concrete security treatment of symmetric encryption: analysis of the DES modes of operation. http://www-cse.ucsd.edu/users/mihir/papers/sym-enc.html, 1997.

[GolBel01] S. Goldwasser, M. Bellare: Lecture notes on cryptography. http://www-cse.ucsd.edu/users/mihir/papers/gb.html, 2001.

[Maurer01] U.M. Maurer et al.: Web pages of the Information Security and Cryptography Research Group, Swiss Federal Institute of Technology (ETH), Zürich, http://www.crypto.ethz.ch/research.

[NIST2000] National Institute of Standards and Technology. Advanced Encryption algorithm (AES) development effort. http://www.nist.gov/aes.

[RSALabs99] RSA Laboratories: DES challenge III. http://www.rsa.com/rsalabs/des3/index.html.