Bibliography

[1] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr. RSA/Rabin Functions: Certain Parts Are as Hard as the Whole. *SIAM Journal on Computing,* Vol. 17, April 1988, pages 194–209.

[2] J. H. An and M. Bellare. Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions. In *Crypto99,* Springer Lecture Notes in Computer Science (Vol. 1666), 1999, pages 252–269.

[3] H. Attiya and J. Welch. *Distributed Computing: Fundamentals, Simulations and Advanced Topics*. London: McGraw-Hill, 1998.

[4] E. Bach and J. Shallit. *Algorithmic Number Theory* (Volume I: Efficient Algorithms). Cambridge, MA: MIT Press, 1996.

[5] B. Barak. How to Go Beyond the Black-Box Simulation Barrier. In *42nd IEEE Symposium on Foundations of Computer Science,* 2001, pages 106–115.

[6] B. Barak. Constant-Round Coin-Tossing with a Man in the Middle or Realizing the Shared Random-String Model. In *43th IEEE Symposium on Foundations of Computer Science,* 2002, pages 345–355.

[7] B. Barak and O. Goldreich. Universal Arguments and Their Applications. In the *17th IEEE Conference on Computational Complexity,* 2002, pages 194–203.

[8] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang. On the (Im)possibility of Software Obfuscation. In *Crypto01,* Springer-Verlag Lecture Notes in Computer Science (Vol. 2139), 2001, pages 1–18.

[9] B. Barak and Y. Lindell. Strict Polynomial-Time in Simulation and Extraction. In *34th ACM Symposium on the Theory of Computing,* 2002, pages 484–493.

[10] D. Beaver. Foundations of Secure Interactive Computing. In *Crypto91*, Springer-Verlag Lecture Notes in Computer Science (Vol. 576), 1992, pages 377–391.

[11] D. Beaver. Secure Multi-Party Protocols and Zero-Knowledge Proof Systems Tolerating a Faulty Minority. *Journal of Cryptology,* Vol. 4, 1991, pages 75–122.

[12] M. Bellare. A Note on Negligible Functions. *Journal of Cryptology,* Vol. 15, 2002, pages 271–284.

[13] M. Bellare, R. Canetti, and H. Krawczyk. Pseudorandom Functions Revisited: The Cascade Construction and Its Concrete Security. In *37th IEEE Symposium on Foundations of Computer Science,* 1996, pages 514–523.

[14] M. Bellare, R. Canetti, and H. Krawczyk. Keying Hash Functions for Message Authentication. In *Crypto96,* Springer Lecture Notes in Computer Science (Vol. 1109), 1996, pages 1–15.

[15] M. Bellare, R. Canetti, and H. Krawczyk. Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols. In *30th ACM Symposium on the Theory of Computing,* 1998, pages 419–428.

[16] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among Notions of Security for Public-Key Encryption Schemes. In *Crypto98,* Springer Lecture Notes in Computer Science (Vol. 1462), 1998, pages 26–45.

[17] M. Bellare and O. Goldreich. On Defining Proofs of Knowledge. In *Crypto92,* Springer-Verlag Lecture Notes in Computer Science (Vol. 740), 1992, pages 390–420.

[18] M. Bellare, O. Goldreich, and S. Goldwasser. Incremental Cryptography: The Case of Hashing and Signing. In *Crypto94,* Springer-Verlag Lecture Notes in Computer Science (Vol. 839), 1994, pages 216–233.

[19] M. Bellare, O. Goldreich, and S. Goldwasser. Incremental Cryptography and Application to Virus Protection. In *27th ACM Symposium on the Theory of Computing,* 1995, pages 45–56.

[20] M. Bellare, O. Goldreich, and H. Krawczyk. Stateless Evaluation of Pseudorandom Functions: Security Beyond the Birthday Barrier. In *Crypto99,* Springer Lecture Notes in Computer Science (Vol. 1666), 1999, pages 270–287.

[21] M. Bellare and S. Goldwasser. New Paradigms for Digital Signatures and Message Authentication Based on Non-Interative Zero-Knowledge Proofs. In *Crypto89,* Springer-Verlag Lecture Notes in Computer Science (Vol. 435), 1990, pages 194–211.

[22] M. Bellare, R. Guerin, and P. Rogaway. XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions. In *Crypto95,* Springer-Verlag Lecture Notes in Computer Science (Vol. 963), 1995, pages 15–28.

[23] M. Bellare, S. Halevi, A. Sahai, and S. Vadhan. Trapdoor Functions and Public-Key Cryptosystems. In *Crypto98,* Springer Lecture Notes in Computer Science (Vol. 1462), 1998, pages 283–298.

[24] M. Bellare, R. Impagliazzo, and M. Naor. Does Parallel Repetition Lower the Error in Computationally Sound Protocols? In *38th IEEE Symposium on Foundations of Computer Science,* 1997, pages 374–383.

[25] M. Bellare, J. Kilian, and P. Rogaway. The Security of Cipher Block Chaining. In *Crypto94,* Springer-Verlag Lecture Notes in Computer Science (Vol. 839), 1994, pages 341–358.

[26] M. Bellare and S. Micali. How to Sign Given Any Trapdoor Function. *Journal of the ACM,* Vol. 39, 1992, pages 214–233.

[27] D. Beaver, S. Micali, and P. Rogaway. The Round Complexity of Secure Protocols. In *22nd ACM Symposium on the Theory of Computing,* 1990, pages 503–513.

[28] M. Bellare and P. Rogaway. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols. In *1st Conf. on Computer and Communications Security,* ACM, 1993, pages 62–73.

[29] M. Bellare and P. Rogaway. Entity Authentication and Key Distribution. In *Crypto93,* Springer-Verlag Lecture Notes in Computer Science (Vol. 773), 1994, pages 232–249.

[30] M. Bellare and P. Rogaway. Provably Secure Session Key Distribution: The Three Party Case. In *27th ACM Symposium on the Theory of Computing,* 1995, pages 57–66.

[31] M. Bellare and P. Rogaway. The Exact Security of Digital Signatures: How to Sign with RSA and Rabin. In *EuroCrypt96,* Springer Lecture Notes in Computer Science (Vol. 1070), 1996, pages 399–416.

[32] M. Bellare and M. Yung. Certifying Permutations: Noninteractive Zero-Knowledge Based on Any Trapdoor Permutation. *Journal of Cryptology,* Vol. 9, 1996, pages 149–166.

[33] M. Ben-Or, R. Canetti, and O. Goldreich. Asynchronous Secure Computation. In *25th ACM Symposium on the Theory of Computing,* 1993, pages 52–61. See details in [49].

[34] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. In *20th ACM Symposium on the Theory of Computing,* 1988, pages 1–10.

[35] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway. UMAC: Fast and Secure Message Authentication. In *Crypto99,* Springer Lecture Notes in Computer Science (Vol. 1666), 1999, pages 216–233.

[36] M. Blum. How to Exchange Secret Keys. *ACM Trans. Comput. Sys.*, Vol. 1, 1983, pages 175–193.

[37] M. Blum. Coin Flipping by Phone. In *the 24th IEEE Computer Conference (CompCon),* February 1982, pages 133–137. See also *SIGACT News,* Vol. 15, No. 1, 1983.

[38] L. Blum, M. Blum, and M. Shub. A Simple Secure Unpredictable Pseudo-Random Number Generator. *SIAM Journal on Computing,* Vol. 15, 1986, pages 364–383.

[39] M. Blum, A. De Santis, S. Micali, and G. Persiano. Non-Interactive Zero-Knowledge Proof Systems. *SIAM Journal on Computing,* Vol. 20, No. 6, 1991, pages 1084–1118. (Considered the journal version of [40].)

[40] M. Blum, P. Feldman, and S. Micali. Non-Interactive Zero-Knowledge and Its Applications. In *20th ACM Symposium on the Theory of Computing,* 1988, pages 103–112. See [39].

[41] M. Blum and S. Goldwasser. An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information. In *Crypto84,* Springer-Verlag Lecture Notes in Computer Science (Vol. 196), 1985, pages 289–302.

[42] M. Blum and S. Micali. How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. *SIAM Journal on Computing,* Vol. 13, 1984, pages 850–864. Preliminary version in *23rd IEEE Symposium on Foundations of Computer Science,* 1982.

[43] J. B. Boyar. Inferring Sequences Produced by Pseudo-Random Number Generators. *Journal of the ACM,* Vol. 36, 1989, pages 129–141.

[44] G. Brassard. A Note on the Complexity of Cryptography. *IEEE Trans. on Inform. Th.,* Vol. 25, 1979, pages 232–233.

[45] G. Brassard. Quantum Information Processing: The Good, the Bad and the Ugly. In *Crypto97,* Springer Lecture Notes in Computer Science (Vol. 1294), 1997 pages 337–341.

[46] G. Brassard, D. Chaum, and C. Crépeau. Minimum Disclosure Proofs of Knowledge. *Journal of Computer and System Science,* Vol. 37, No. 2, 1988, pages 156–189. Preliminary version by Brassard and Crépeau in *27th IEEE Symposium on Foundations of Computer Science,* 1986.

[47] G. Brassard, C. Crépeau, and M. Yung. Constant-Round Perfect Zero-Knowledge Computationally Convincing Protocols. *Theoretical Computer Science,* Vol. 84, 1991, pages 23–52.

[48] C. Cachin and U. Maurer. Unconditional Security Against Memory-Bounded Adversaries. In *Crypto97,* Springer Lecture Notes in Computer Science (Vol. 1294), 1997, pages 292–306.

[49] R. Canetti. *Studies in Secure Multi-Party Computation and Applications*. Ph.D. thesis, Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel, June 1995. Available from `http://theory.lcs.mit.edu/~tcryptol/BOOKS/ran-phd.html`.

[50] R. Canetti. Security and Composition of Multi-party Cryptographic Protocols. *Journal of Cryptology,* Vol. 13, No. 1, 2000, pages 143–202.

[51] R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *42nd IEEE Symposium on Foundations of Computer Science,* 2001, pages 136–145. Full version (with different title) is available from *Cryptology ePrint Archive,* Report 2000/067.

[52] R. Canetti, I. Damgard, S. Dziembowski, Y. Ishai, and T. Malkin. On Adaptive Versus Non-Adaptive Security of Multiparty Protocols. *Journal of Cryptology,* forthcoming.

[53] R. Canetti, U. Feige, O. Goldreich, and M. Naor. Adaptively Secure Multiparty Computation. In *28th ACM Symposium on the Theory of Computing,* 1996, pages 639–648.

[54] R. Canetti, O. Goldreich, and S. Halevi. The Random Oracle Methodology, Revisited. In *30th ACM Symposium on the Theory of Computing,* 1998, pages 209–218.

[55] R. Canetti, O. Goldreich, S. Goldwasser, and S. Micali. Resettable Zero-Knowledge. In *32nd ACM Symposium on the Theory of Computing,* 2000, pages 235–244.

[56] R. Canetti, S. Halevi, and A. Herzberg. How to Maintain Authenticated Communication in the Presence of Break-Ins. *Journal of Cryptology,* Vol. 13, No. 1, 2000, pages 61–106.

[57] R. Canetti and A. Herzberg. Maintaining Security in the Presence of Transient Faults. In *Crypto94,* Springer-Verlag Lecture Notes in Computer Science (Vol. 839), 1994, pages 425–439.

[58] R. Canetti, J. Kilian, E. Petrank, and A. Rosen. Black-Box Concurrent Zero-Knowledge Requires $\tilde{\Omega}(\log n)$ Rounds. In *33rd ACM Symposium on the Theory of Computing,* 2001, pages 570–579.

[59] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally Composable Two-Party and Multi-Party Secure Computation. In *34th ACM Symposium on the Theory of Computing,* 2002, pages 494–503.

[60] L. Carter and M. Wegman. Universal Hash Functions. *Journal of Computer and System Science,* Vol. 18, 1979, pages 143–154.

[61] D. Chaum. Blind Signatures for Untraceable Payments. In *Crypto82*. New York: Plenum Press, 1983, pages 199–203.

[62] D. Chaum, C. Crépeau, and I. Damgård. Multi-party Unconditionally Secure Protocols. In *20th ACM Symposium on the Theory of Computing,* 1988, pages 11–19.

[63] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. In *26th IEEE Symposium on Foundations of Computer Science,* 1985, pages 383–395.

[64] B. Chor and E. Kushilevitz. A Zero-One Law for Boolean Privacy. *SIAM J. on Disc. Math.,* Vol. 4, 1991, pages 36–47.

[65] R. Cleve. Limits on the Security of Coin Flips When Half the Processors Are Faulty. In *18th ACM Symposium on the Theory of Computing,* 1986, pages 364–369.

[66] J. D. Cohen and M. J. Fischer. A Robust and Verifiable Cryptographically Secure Election Scheme. In *26th IEEE Symposium on Foundations of Computer Science,* 1985, pages 372–382.

[67] R. Cramer and I. Damgård. New Generation of Secure and Practical RSA-Based Signatures. In *Crypto96,* Springer Lecture Notes in Computer Science (Vol. 1109), 1996, pages 173–185.

[68] R. Cramer and V. Shoup. A Practical Public-Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attacks. In *Crypto98,* Springer-Verlag Lecture Notes in Computer Science (Vol. 1462), 1998, pages 13–25.

[69] C. Crépeau. Efficient Cryptographic Protocols Based on Noisy Channels. In *EuroCrypt97,* Springer, Lecture Notes in Computer Science (Vol. 1233), 1997, pages 306–317.

[70] I. Damgård. Collision Free Hash Functions and Public Key Signature Schemes. In *EuroCrypt87,* Springer-Verlag Lecture Notes in Computer Science (Vol. 304), 1988, pages 203–216.

[71] I. Damgård. A Design Principle for Hash Functions. In *Crypto89,* Springer-Verlag Lecture Notes in Computer Science (Vol. 435), 1990, pages 416–427.

[72] I. Damgård. Concurrent Zero-Knowledge in Easy in Practice: Theory of Cryptography Library, 99-14, June 1999. `http://philby.ucsd.edu/cryptolib`. See also "Efficient Concurrent Zero-Knowledge in the Auxiliary String Model" (in *Eurocrypt'00,* 2000).

[73] A. De Santis, G. Di Crescenzo, R. Ostrovsky, G. Persiano, and A. Sahai. Robust Non-interactive Zero-Knowledge. In *Crypto01,* Springer Lecture Notes in Computer Science (Vol. 2139), 2001, pages 566–598.

[74] Y. Desmedt and Y. Frankel. Threshold Cryptosystems. In *Crypto89,* Springer-Verlag Lecture Notes in Computer Science (Vol. 435), 1990, pages 307–315.

[75] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Trans. on Info. Theory,* IT-22, Nov. 1976, pages 644–654.

[76] H. Dobbertin. The Status of MD5 after a Recent Attack. In *CryptoBytes,* RSA Lab., Vol. 2, No. 2, 1996, pages 1–6.

[77] D. Dolev, C. Dwork, and M. Naor. Non-Malleable Cryptography. In *23rd ACM Symposium on the Theory of Computing,* 1991, pages 542–552. Full version available from authors.

[78] D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly Secure Message Transmission. *Journal of the ACM,* Vol. 40 (1), 1993, pages 17–47.

[79] D. Dolev and A. C. Yao. On the Security of Public-Key Protocols. *IEEE Trans. on Inform. Theory,* Vol. 30, No. 2, 1983, pages 198–208.

[80] D. Dolev and H. R. Strong. Authenticated Algorithms for Byzantine Agreement. *SIAM Journal on Computing,* Vol. 12, 1983, pages 656–666.

[81] C. Dwork and M. Naor. An Efficient Existentially Unforgeable Signature Scheme and Its Application. *Journal of Cryptology,* Vol. 11 (3), 1998, pages 187–208

[82] C. Dwork, M. Naor, and A. Sahai. Concurrent Zero-Knowledge. In *30th ACM Symposium on the Theory of Computing,* 1998, pages 409–418.

[83] S. Even and O. Goldreich. On the Security of Multi-party Ping-Pong Protocols. In *24th IEEE Symposium on Foundations of Computer Science,* 1983, pages 34–39.

[84] S. Even, O. Goldreich, and A. Lempel. A Randomized Protocol for Signing Contracts. *CACM,* Vol. 28, No. 6, 1985, pages 637–647.

[85] S. Even, O. Goldreich, and S. Micali. On-line/Off-line Digital Signatures. *Journal of Cryptology,* Vol. 9, 1996, pages 35–67.

[86] S. Even, A.L. Selman, and Y. Yacobi. The Complexity of Promise Problems with Applications to Public-Key Cryptography. *Information and Control,* Vol. 61, 1984, pages 159–173.

[87] S. Even and Y. Yacobi. Cryptography and NP-Completeness. *In Proceedings of 7th ICALP,* Springer-Verlag Lecture Notes in Computer Science (Vol. 85), 1980, pages 195–207. See [86].

[88] U. Feige, A. Fiat, and A. Shamir. Zero-Knowledge Proofs of Identity. *Journal of Cryptology,* Vol. 1, 1988, pages 77–94.

[89] U. Feige, D. Lapidot, and A. Shamir. Multiple Non-Interactive Zero-Knowledge Proofs under General Assumptions. *SIAM Journal on Computing,* Vol. 29 (1), 1999, pages 1–28.

[90] U. Feige and A. Shamir. Zero-Knowledge Proofs of Knowledge in Two Rounds. In *Crypto89,* Springer-Verlag Lecture Notes in Computer Science (Vol. 435), 1990, pages 526–544.

[91] U. Feige and A. Shamir. Witness Indistinguishability and Witness Hiding Protocols. In *22nd ACM Symposium on the Theory of Computing,* 1990, pages 416–426.

[92] A. Fiat and A. Shamir. How to Prove Yourself: Practical Solution to Identification and Signature Problems. In *Crypto86,* Springer-Verlag Lecture Notes in Computer Science (Vol. 263), 1987, pages 186–189.

[93] M. Fischer, S. Micali, C. Rackoff, and D. K. Wittenberg. An Oblivious Transfer Protocol Equivalent to Factoring. Unpublished manuscript, 1986. Preliminary versions were presented in *EuroCrypt84* and in the *NSF Workshop on Mathematical Theory of Security,* Endicott House, 1985.

[94] A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias, and A. Shamir. Reconstructing Truncated Integer Variables Satisfying Linear Congruences. *SIAM Journal on Computing,* Vol. 17, 1988, pages 262–280.

[95] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York: W. H. Freeman and Company, 1979.

[96] P. S. Gemmell. An Introduction to Threshold Cryptography. In *CryptoBytes,* RSA Lab., Vol. 2, No. 3, 1997, pages 7–12.

[97] R. Gennaro, M. Rabin, and T. Rabin. Simplified VSS and Fast-Track Multiparty Computations with Applications to Threshold Cryptography. In *17th ACM Symposium on Principles of Distributed Computing,* 1998, pages 101–112.

[98] R. Gennaro and L. Trevisan. Lower Bounds on the Efficiency of Generic Cryptographic Constructions. In *41st Symposium on Foundations of Computer Science,* 2000, pages 305–313.

[99] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane. Codes Which Detect Deception. *Bell Syst. Tech. J.,* Vol. 53, 1974, pages 405–424.

[100] O. Goldreich. Two Remarks Concerning the GMR Signature Scheme. In *Crypto86,* Springer-Verlag Lecture Notes in Computer Science (Vol. 263), 1987, pages 104–110.

[101] O. Goldreich. *Foundation of Cryptography – Class Notes*. Preprint, Spring 1989. See [102]. Superseded by the current work.

[102] O. Goldreich. *Lecture Notes on Encryption, Signatures and Cryptographic Protocol*. Extracts from [101]. Available from `http://www.wisdom.weizmann.ac.il/~oded/foc.html`. Superseded by the current work.

[103] O. Goldreich. A Note on Computational Indistinguishability. *Information Processing Letters,* Vol. 34, May 1990, pages 277–281.

[104] O. Goldreich. A Uniform Complexity Treatment of Encryption and Zero-Knowledge. *Journal of Cryptology,* Vol. 6, No. 1, 1993, pages 21–53.

[105] O. Goldreich. *Foundation of Cryptography – Fragments of a Book*. February 1995. Available from `http://www.wisdom.weizmann.ac.il/~oded/foc.html`. Superseded by the current work.

[106] O. Goldreich. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Algorithms and Combinatorics series, Vol. 17. Heidelberg: Springer, 1999.

[107] O. Goldreich. *Secure Multi-Party Computation*. Unpublished manuscript, 1998. Available from `http://www.wisdom.weizmann.ac.il/~oded/foc.html`. Superseded by the current work.

[108] O. Goldreich. *Foundation of Cryptography – Basic Tools*. New York: Cambridge University Press, 2001.

[109] O. Goldreich. Concurrent Zero-Knowledge With Timing, Revisited. In *34th ACM Symposium on the Theory of Computing,* 2002, pages 332–340.

[110] O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions. *Journal of the ACM,* Vol. 33, No. 4, 1986, pages 792–807.

[111] O. Goldreich, S. Goldwasser, and S. Micali. On the Cryptographic Applications of Random Functions. In *Crypto84,* Springer-Verlag Lecture Notes in Computer Science (Vol. 263), 1985, pages 276–288.

[112] O. Goldreich and A. Kahan. How to Construct Constant-Round Zero-Knowledge Proof Systems for NP. *Journal of Cryptology,* Vol. 9, No. 2, 1996, pages 167–189. Preliminary versions date to 1988.

[113] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. *SIAM Journal on Computing,* Vol. 25, No. 1, February 1996, pages 169–192.

[114] O. Goldreich and L. A. Levin. Hard-Core Predicates for Any One-Way Function. In *21st ACM Symposium on the Theory of Computing,* 1989, pages 25–32.

[115] O. Goldreich and Y. Lindell. Session-Key Generation Using Human Passwords. In *Crypto01,* Springer-Verlag Lecture Notes in Computer Science (Vol. 2139), 2001, pages 408–432.

[116] O. Goldreich, Y. Lustig, and M. Naor. On Chosen Ciphertext Security of Multiple Encryptions. *Cryptology ePrint Archive,* Report 2002/089, 2002.

[117] O. Goldreich, S. 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,* Vol. 38, No. 1, 1991, pages 691–729. Preliminary version in *27th IEEE Symposium on Foundations of Computer Science,* 1986.

[118] O. Goldreich, S. Micali, and A. Wigderson. How to Play Any Mental Game – A Completeness Theorem for Protocols with Honest Majority. In *19th ACM Symposium on the Theory of Computing,* 1987, pages 218–229.

[119] O. Goldreich and Y. Oren. Definitions and Properties of Zero-Knowledge Proof Systems. *Journal of Cryptology,* Vol. 7, No. 1, 1994, pages 1–32.

[120] O. Goldreich and R. Vainish. How to Solve Any Protocol Problem – An Efficiency Improvement. In *Crypto87,* Springer Verlag Lecture Notes in Computer Science (Vol. 293), 1988, pages 73–86.

[121] S. Goldwasser and L. A. Levin. Fair Computation of General Functions in Presence of Immoral Majority. In *Crypto90,* Springer-Verlag Lecture Notes in Computer Science (Vol. 537), 1991, pages 77–93.

[122] S. Goldwasser and Y. Lindell. Secure Computation Without Agreement. In *16th International Symposium on Distributed Computing* (DISC), Springer-Verlag Lecture Notes in Computer Science (Vol. 2508), 2002, pages 17–32.

[123] S. Goldwasser and S. Micali. Probabilistic Encryption. *Journal of Computer and System Science,* Vol. 28, No. 2, 1984, pages 270–299. Preliminary version in *14th ACM Symposium on the Theory of Computing,* 1982.

[124] S. Goldwasser, S. Micali, and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing,* Vol. 18, 1989, pages 186–208. Preliminary version in *17th ACM Symposium on the Theory of Computing,* 1985.

[125] S. Goldwasser, S. Micali, and R. L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. *SIAM Journal on Computing,* Vol. 17, No. 2, April 1988, pages 281–308.

[126] S. Goldwasser, S. Micali, and P. Tong. Why and How to Establish a Private Code in a Public Network. In *23rd IEEE Symposium on Foundations of Computer Science,* 1982, pages 134–144.

[127] S. Goldwasser, S. Micali, and A. C. Yao. Strong Signature Schemes. In *15th ACM Symposium on the Theory of Computing,* 1983, pages 431–439.

[128] S. Goldwasser and R. Ostrovsky. Invariant Signatures and Non-Interactive Zero-Knowledge Proofs Are Equivalent. In *Crypto92,* Springer-Verlag Lecture Notes in Computer Science (Vol. 740), 1992, pages 228–245.

[129] S. Haber and S. Micali. Private communication, 1986.

[130] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A Pseudorandom Generator from Any One-way Function. *SIAM Journal on Computing,* Vol. 28, No. 4, 1999, pages 1364–1396. Preliminary versions by Impagliazzo et al. in *21st ACM Symposium on the Theory of Computing* (1989) and Håstad in *22nd ACM Symposium on the Theory of Computing* (1990).

[131] M. Hirt and U. Maurer. Complete Characterization of Adversaries Tolerable in Secure Multi-party Computation. *Journal of Cryptology,* Vol. 13, No. 1, 2000, pages 31–60.

[132] R. Impagliazzo and M. Luby. One-Way Functions Are Essential for Complexity Based Cryptography. In *30th IEEE Symposium on Foundations of Computer Science,* 1989, pages 230–235.

[133] R. Impagliazzo and S. Rudich. Limits on the Provable Consequences of One-Way Permutations. In *21st ACM Symposium on the Theory of Computing,* 1989, pages 44–61.

[134] A. Juels, M. Luby, and R. Ostrovsky. Security of Blind Digital Signatures. In *Crypto97,* Springer-Verlag Lecture Notes in Computer Science (Vol. 1294), 1997, pages 150–164.

[135] J. Kahn, M. Saks, and C. Smyth. A Dual Version of Reimer's Inequality and a Proof of Rudich's Conjecture. In *15th IEEE Conference on Computational Complexity,* 2000, pages 98–103.

[136] J. Katz and M. Yung. Complete Characterization of Security Notions for Probabilistic Private-Key Encryption. In *32nd ACM Symposium on the Theory of Computing,* 2000, pages 245–254.

[137] J. Kilian. Basing Cryptography on Oblivious Transfer. In *20th ACM Symposium on the Theory of Computing,* 1988, pages 20–31.

[138] J. Kilian and E. Petrank. Concurrent and Resettable Zero-Knowledge in Poly-logarithmic Rounds. In *33rd ACM Symposium on the Theory of Computing,* 2001, pages 560–569.

[139] H. Krawczyk. LFSR-Based Hashing and Authentication. In *Crypto94,* Springer-Verlag Lecture Notes in Computer Science (Vol. 839), 1994, pages 129–139.

[140] H. Krawczyk. New Hash Functions For Message Authentication. In *EuroCrypt95*, Springer-Verlag Lecture Notes in Computer Science (Vol. 921), 1995, pages 301–310.

[141] A. Lempel. Cryptography in Transition. *Computing Surveys,* Vol. 11, No. 4, Dec. 1979, pages 285–303.

[142] Y. Lindell. A Simpler Construction of CCA2-Secure Public-Key Encryption under General Assumptions. In *EuroCrypt03*, Springer Lecture Notes in Computer Science (Vol. 2656), 2003, pages 241–254.

[143] Y. Lindell. Parallel Coin-Tossing and Constant-Round Secure Two-Party Computation. In *Crypto01*, Springer Lecture Notes in Computer Science (Vol. 2139), 2001, pages 171–189.

[144] Y. Lindell, A. Lysyanskaya, and T. Rabin. On the Composition of Authenticated Byzantine Agreement. In *34th ACM Symposium on the Theory of Computing,* 2002, pages 514–523.

[145] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton, NJ: Princeton University Press, 1996.

[146] M. Luby and C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing,* Vol. 17, 1988, pages 373–386.

[147] N. Lynch. *Distributed Algorithms*. San Mateo, CA: Morgan Kaufmann Publishers, 1996.

[148] U. Maurer. Secret Key Agreement by Public Discussion from Common Information. *IEEE Trans. on Inform. Th.,* Vol. 39, No. 3, May 1993, pages 733–742.

[149] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996.

[150] R. C. Merkle. Secure Communication over Insecure Channels. *CACM,* Vol. 21, No. 4, 1978, pages 294–299.

[151] R. C. Merkle. Protocols for Public Key Cryptosystems. In *Proceedings of the 1980 Symposium on Security and Privacy,* 1980, pages 122–134.

[152] R. C. Merkle. A Digital Signature Based on a Conventional Encryption Function. In *Crypto87,* Springer-Verlag Lecture Notes in Computer Science (Vol. 293), 1987, pages 369–378.

[153] R. C. Merkle. A Certified Digital Signature Scheme. In *Crypto89,* Springer-Verlag Lecture Notes in Computer Science (Vol. 435), 1990, pages 218–238.

[154] R. C. Merkle and M. E. Hellman. Hiding Information and Signatures in Trapdoor Knapsacks. *IEEE Trans. Inform. Theory,* Vol. 24, 1978, pages 525–530.

[155] S. Micali, M. O. Rabin, and S. Vadhan. Verifiable Random Functions. In *40th IEEE Symposium on Foundations of Computer Science,* 1999, pages 120–130.

[156] S. Micali, C. Rackoff, and B. Sloan. The Notion of Security for Probabilistic Cryptosystems. *SIAM Journal on Computing,* Vol. 17, 1988, pages 412–426.

[157] S. Micali and P. Rogaway. Secure Computation. In *Crypto91,* Springer-Verlag Lecture Notes in Computer Science (Vol. 576), 1992, pages 392–404.

[158] D. Micciancio. Oblivious Data Structures: Applications to Cryptography. In *29th ACM Symposium on the Theory of Computing,* 1997, pages 456–464.

[159] National Bureau of Standards. Data Encryption Standard (DES). *Federal Information Processing Standards,* Publ. 46, 1977.

[160] National Institute for Standards and Technology. Digital Signature Standard (DSS). *Federal Register,* Vol. 56, No. 169, Aug. 1991.

[161] M. Naor. Bit Commitment Using Pseudorandom Generators. *Journal of Cryptology,* Vol. 4, 1991, pages 151–158.

[162] M. Naor and O. Reingold. From Unpredictability to Indistinguishability: A Simple Construction of Pseudorandom Functions from MACs. In *Crypto98,* Springer-Verlag Lecture Notes in Computer Science (Vol. 1464), 1998, pages 267–282.

[163] M. Naor and M. Yung. Universal One-Way Hash Functions and their Cryptographic Application. *21st ACM Symposium on the Theory of Computing,* 1989, pages 33–43.

[164] M. Naor and M. Yung. Public-Key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks. In *22nd ACM Symposium on the Theory of Computing,* 1990, pages 427–437.

[165] R. Ostrovsky, R. Venkatesan, and M. Yung. Secure Commitment Against Powerful Adversary: A Security Primitive Based on Average Intractability. In *Proceedings of the 9th Symposium on Theoretical Aspects of Computer Science (STACS92),* 1992, pages 439–448.

[166] R. Ostrovsky and M. Yung. How to Withstand Mobile Virus Attacks. In *10th ACM Symposium on Principles of Distributed Computing,* 1991, pages 51–59.

[167] T. P. Pedersen and B. Pfitzmann. Fail-Stop Signatures. *SIAM Journal on Computing,* Vol. 26, No. 2, 1997, pages 291–330. Based on several earlier works (see first footnote in the paper).

[168] B. Pfitzmann. *Digital Signature Schemes* (*General Framework and Fail-Stop Signatures*). Springer-Verlag Lecture Notes in Computer Science (Vol. 1100), 1996.

[169] M. Prabhakaran, A. Rosen, and A. Sahai. Concurrent Zero-Knowledge Proofs in Logarithmic Number of Rounds. In *43rd IEEE Symposium on Foundations of Computer Science,* 2002, pages 366–375.

[170] M. O. Rabin. Digitalized Signatures. In *Foundations of Secure Computation,* R. A. DeMillo et al., eds. New York: Academic Press, 1977, pages 155–168.

[171] M. O. Rabin. Digitalized Signatures and Public Key Functions as Intractable as Factoring. TR-212, LCS, MIT, 1979.

[172] M. O. Rabin. How to Exchange Secrets by Oblivious Transfer. Tech. Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[173] T. Rabin and M. Ben-Or. Verifiable Secret Sharing and Multi-party Protocols with Honest Majority. In *21st ACM Symposium on the Theory of Computing,* 1989, pages 73–85.

[174] C. Rackoff and D. R. Simon. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In *Crypto91,* Springer Verlag Lecture Notes in Computer Science (Vol. 576), 1991, pages 433–444.

[175] R. Richardson and J. Kilian. On the Concurrent Composition of Zero-Knowledge Proofs. In *EuroCrypt99,* Springer-Verlag Lecture Notes in Computer Science (Vol. 1592), 1999, pages 415–413.

[176] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *CACM,* Vol. 21, Feb. 1978, pages 120–126.

[177] P. Rogaway. The Round Complexity of Secure Protocols. Ph.D. thesis, MIT June 1991. Available from `http://www.cs.ucdavis.edu/~rogaway/papers`.

[178] J. Rompel. One-Way Functions Are Necessary and Sufficient for Secure Signatures. In *22nd ACM Symposium on the Theory of Computing,* 1990, pages 387–394.

[179] A. Sahai. Non-Malleable Non-Interactive Zero Knowledge and Achieving Chosen-Ciphertext Security. In *40th IEEE Symposium on Foundations of Computer Science,* 1999, pages 543–553.

[180] A. Sahai. Improved Constructions Achieving Chosen-Ciphertext Security. Unpublished manuscript, 2001. See [73].

[181] A. Shamir. On the Cryptocomplexity of Knapsack systems. In *11th ACM Symposium on the Theory of Computing,* 1979, pages 118–129.

[182] A. Shamir. How to Share a Secret. *CACM,* Vol. 22, Nov. 1979, pages 612–613.

[183] A. Shamir. A Polynomial-Time Algorithm for Breaking the Merkle-Hellman Cryptosystem. In *23rd IEEE Symposium on Foundations of Computer Science,* 1982, pages 145–152.

[184] A. Shamir, R. L. Rivest, and L. Adleman. Mental Poker. TM-125, LCS, MIT, 1979.

[185] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal,* Vol. 28, 1949, pages 656–715.

[186] D. Stinson. Universal Hashing and Authentication Codes. *Designs, Codes and Cryptography,* Vol. 4, 1994, pages 369–380.

[187] S. Vadhan. Constructing Locally Computable Extractors and Cryptosystems in the Bounded Storage Model. *Journal of Cryptology*, Vol. 17, No. 1, 2004, pages 43–77.

[188] M. Wegman and L. Carter. New Hash Functions and Their Use in Authentication and Set Equality. *Journal of Computer and System Science,* Vol. 22, 1981, pages 265–279.

[189] A. D. Wyner. The Wire-Tap Channel. *Bell System Technical Journal*, Vol. 54, No. 8, Oct. 1975, pages 1355–1387.

[190] A. C. Yao. Theory and Application of Trapdoor Functions. In *23rd IEEE Symposium on Foundations of Computer Science,* 1982, pages 80–91.

[191] A. C. Yao. How to Generate and Exchange Secrets. In *27th IEEE Symposium on Foundations of Computer Science,* 1986, pages 162–167.