Bibliography

[1] W. Aiello, M. Bellare and R. Venkatesan. Knowledge on the Average – Perfect, Statistical and Logarithmic. In *27th ACM Symposium on the Theory of Computing*, pages 469–478, 1995.

[2] W. Aiello and J. Håstad. Perfect Zero-Knowledge Languages can be Recognized in Two Rounds. In *28th IEEE Symposium on Foundations of Computer Science*, pages 439–448, 1987.

[3] M. Ajtai. Generating Hard Instances of Lattice Problems. In *28th ACM Symposium on the Theory of Computing*, pages 99–108, 1996.

[4] M. Ajtai, J. Komlos, E. Szemerédi. Deterministic Simulation in LogSpace. In *19th ACM Symposium on the Theory of Computing*, pages 132–140, 1987.

[5] M. Ajtai and A. Wigderson. Deterministic simulation of probabilistic constant depth circuits. In *26th IEEE Symposium on Foundations of Computer Science*, pages 11–19, 1985.

[6] R. Aleliunas, R.M. Karp, R.J. Lipton, L. Lovász and C. Rackoff. Random walks, universal traversal sequences, and the complexity of maze problems. In *20th IEEE Symposium on Foundations of Computer Science*, pages 218–223, 1979.

[7] 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.

[8] N. Alon. Eigenvalues and expanders. *Combinatorica*, Vol. 6, pages 83–96, 1986.

[9] N. Alon, L. Babai and A. Itai. A fast and Simple Randomized Algorithm for the Maximal Independent Set Problem. *J. of Algorithms*, Vol. 7, pages 567–583, 1986.

[10] N. Alon, J. Bruck, J. Naor, M. Naor and R. Roth. Construction of Asymptotically Good, Low-Rate Error-Correcting Codes through Pseudo-Random Graphs. *IEEE Transactions on Information Theory*, Vol. 38, pages 509–516, 1992.

[11] N. Alon, O. Goldreich, J. Håstad, R. Peralta. Simple Constructions of Almost k-wise Independent Random Variables. *Journal of Random structures and Algorithms*, Vol. 3, No. 3, (1992), pages 289–304.

[12] N. Alon and V.D. Milman. λ_1, Isoperimetric Inequalities for Graphs and Superconcentrators, *J. Combinatorial Theory, Ser. B*, Vol. 38, pages 73–88, 1985.

[13] N. Alon and J.H. Spencer. *The Probabilistic Method*, John Wiley & Sons, Inc., 1992.

[14] A.E. Andreev, A.E.F. Clementi, J.D.P. Rolin and L. Trevisan, Weak Random Sources, Hitting Sets, and BPP Simulations. To appear in *SIAM Journal on Computing*. Preliminary version in *38th IEEE Symposium on Foundations of Computer Science*, pages 264–272, 1997.

[15] R. Armoni, M. Saks, A. Wigderson and S. Zhou. Discrepancy sets and pseudorandom generators for combinatorial rectangles. In *37th IEEE Symposium on Foundations of Computer Science*, pages 412-421, 1996.

[16] R. Armoni, A. Ta-Shma, A. Wigderson and S. Zhou. $SL \subseteq L^{4/3}$. In *29th ACM Symposium on the Theory of Computing*, pages 230–239, 1997.

[17] R. Armoni and A. Wigderson. Pseudorandomness for space-bounbded computation. Unpublished manuscript, 1995.

[18] S. Arora and C. Lund. Hardness of Approximations. In *Approximation Algorithms for NP-hard Problems*, D. Hochbaum ed., PWS, 1996.

[19] S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy. Proof Verification and Intractability of Approximation Problems. *Journal of the ACM*, Vol. 45, pages 501–555, 1998. Preliminary version in *33rd IEEE Symposium on Foundations of Computer Science*, 1992.

[20] S. Arora and S. Safra. Probabilistic Checkable Proofs: A New Characterization of NP. *Journal of the ACM*, Vol. 45, pages 70–122, 1998. Preliminary version in *33rd IEEE Symposium on Foundations of Computer Science*, 1992.

[21] S. Arora and S. Sudan. Improved low degree testing and its applications. In *29th ACM Symposium on the Theory of Computing*, pages 485–495, 1997.

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

[23] L. Babai. Trading Group Theory for Randomness. In *17th ACM Symposium on the Theory of Computing*, pages 421–429, 1985.

[24] L. Babai, L. Fortnow, and C. Lund. Non-Deterministic Exponential Time has Two-Prover Interactive Protocols. *Computational Complexity*, Vol. 1, No. 1, pages 3–40, 1991. Preliminary version in *31st IEEE Symposium on Foundations of Computer Science*, 1990.

[25] L. Babai, L. Fortnow, L. Levin, and M. Szegedy. Checking Computations in Polylogarithmic Time. In *23rd ACM Symposium on the Theory of Computing*, pages 21–31, 1991.

[26] L. Babai, L. Fortnow, N. Nisan and A. Wigderson. BPP has Subexponential Time Simulations unless EXPTIME has Publishable Proofs. *Complexity Theory*, Vol. 3, pages 307–318, 1993.

[27] L. Babai and S. Moran. Arthur-Merlin Games: A Randomized Proof System and a Hierarchy of Complexity Classes. *Journal of Computer and System Science*, Vol. 36, pp. 254–276, 1988.

[28] L. Babai, N. Nisan and M. Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *Journal of Computer and System Science*, Vol. 45(2), pgaes 204–232, 1992.

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

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

[31] D. Beaver and J. Feigenbaum. Hiding Instances in Multioracle Queries. In *7th STACS*, Springer Verlag, Lecture Notes in Computer Science (Vol. 415), pages 37–48, 1990.

[32] 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*, pages 514–523, 1996.

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

[34] 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*, pages 419–428, 1998.

[35] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Crypto98*,

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

[37] M. Bellare, O. Goldreich, and S. Goldwasser. Randomness in Interactive Proofs. *Computational Complexity*, Vol. 4, No. 4, pages 319–354, 1993.

[38] 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), pages 216–233, 1994.

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

[40] M. Bellare, O. Goldreich and M. Sudan. Free Bits, PCPs and Non-Approximability – Towards Tight Results. *SIAM Journal on Computing*, Vol. 27, No. 3, pages 804–915, 1998.

[41] M. Bellare and S. Goldwasser. The Complexity of Decision versus Search. *SIAM Journal on Computing*, Vol. 23, pages 97–119, 1994.

[42] M. Bellare, S. Goldwasser, C. Lund and A. Russell. Efficient probabilistically checkable proofs and applications to approximation. In *25th ACM Symposium on the Theory of Computing*, pages 294–304, 1993.

[43] M. Bellare, S. Goldwasser and D. Micciancio. "Pseudo-random" Number Generation within Cryptographic Algorithms: the DSS Case. In *Crypto97*, Springer Lecture Notes in Computer Science (Vol. 1294), pages 277–291.

[44] 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), pages 15–28.

[45] M. Bellare, S. Halevi, A. Sahai and S. Vadhan. Trapdoor Functions and Public-Key Cryptosystems. In *Crypto98*,

[46] 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*, pages 374–383, 1997.

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

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

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

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

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

[52] 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), pages 399–416.

[53] M. Bellare and J. Rompel. Randomness-efficient oblivious sampling. In *35th IEEE Symposium on Foundations of Computer Science*, pages 276–287, 1994.

[54] M. Bellare and M. Sudan. Improved non-approximability results. In *26th ACM Symposium on the Theory of Computing*, pages 184–193, 1994.

[55] C.H. Bennett, G. Brassard and J.M. Robert. Privacy Amplification by Public Discussion. *SIAM Journal on Computing*, Vol. 17, pages 210–229, 1988. Preliminary version in *Crypto85*, Springer-Verlag Lecture Notes in Computer Science (Vol. 218), pages 468–476 (titled "How to Reduce your Enemy's Information").

[56] M. Ben-Or. Another advantage of free choice: Completely Asynchronous Byzantine Agreement. In *2nd ACM Symposium on Principles of Distributed Computing*, pages 27–30, 1983.

[57] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali and P. Rogaway. Everything Provable is Probable in Zero-Knowledge. In *Crypto88*, Springer-Verlag Lecture Notes in Computer Science (Vol. 403), pages 37–56, 1990

[58] M. Ben-Or, S. Goldwasser, J. Kilian and A. Wigderson. Multi-Prover Interactive Proofs: How to Remove Intractability. In *20th ACM Symposium on the Theory of Computing*, pages 113–131, 1988.

[59] 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*, pages 1–10, 1988.

[60] G.R. Blakley. Safeguarding Cryptographic Keys. In *Proc. of National Computer Conf.*, Vol. 48, AFIPS Press, pages 313–317, 1979.

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

[62] M. Blum. Coin Flipping by Phone. *IEEE Spring COMPCOM*, pages 133–137, February 1982. See also *SIGACT News*, Vol. 15, No. 1, 1983.

[63] 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.

[64] M. Blum, A. De Santis, S. Micali, and G. Persiano. Non-Interactive Zero-Knowledge Proof Systems. *SIAM Journal on Computing*, Vol. 20, No. 6, pages 1084–1118, 1991. (Considered the journal version of [66].)

[65] M. Blum, W. Evans, P. Gemmell, S. Kannan and M. Naor. Checking the correctness of memories. In *32nd IEEE Symposium on Foundations of Computer Science*, pages 90-99, 1991.

[66] M. Blum, P. Feldman and S. Micali. Non-Interactive Zero-Knowledge and its Applications. In *20th ACM Symposium on the Theory of Computing*, pages 103–112, 1988. See [64].

[67] M. Blum and O. Goldreich. Towards a Computational Theory of Statistical Tests. In *33rd IEEE Symposium on Foundations of Computer Science*, pages 406–416, 1992.

[68] M. Blum and S. Goldwasser. An Efficient Probabilistic Public-Key Encryption Scheme which hides all partial information. In *Crypto84*, Lecture Notes in Computer Science (Vol. 196) Springer-Verlag, pages 289–302.

[69] M. Blum, M. Luby and R. Rubinfeld. Self-Testing/Correcting with Applications to Numerical Problems. *Journal of Computer and System Science*, Vol. 47, No. 3, pages 549–595, 1993.

[70] M. Blum and S. Kannan. Designing Programs that Check their Work. In *21st ACM Symposium on the Theory of Computing*, pages 86–97, 1989.

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

[72] D. Boneh, R. DeMillo and R. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In *EuroCrypt97*, Springer Lecture Notes in Computer Science (Vol. 1233), pages 37–51, 1997.

[73] R. Boppana, J. Håstad, and S. Zachos. Does Co-NP Have Short Interactive Proofs? *Information Processing Letters*, 25, May 1987, pp. 127-132.

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

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

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

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

[78] G. Brassard and C. Crépeau. Zero-Knowledge Simulation of Boolean Circuits. In *Crypto86*, Springer-Verlag Lecture Notes in Computer Science (Vol. 263), pages 223–233, 1987.

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

[80] C. Cachin and U. Maurer. Unconditional security against memory-bounded adversaries. In *Crypto97*, Springer Lecture Notes in Computer Science (Vol. 1294), pages 292–306.

[81] 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`.

[82] R. Canetti. Towards Realizing Random Oracles: Hash Functions that Hide All Partial Information. In *Crypto97*, Springer Lecture Notes in Computer Science (Vol. 1294), pages 455–469.

[83] R. Canetti. Security and Composition of Multi-party Cryptographic Protocols. Record 98-18 of the *Theory of Cryptography Library*, URL `http://theory.lcs.mit.edu/~tcryptol`. June 1998.

[84] R. Canetti, C. Dwork, M. Naor and R. Ostrovsky. Deniable Encryption. In *Crypto97*, Springer Lecture Notes in Computer Science (Vol. 1294), pages 90–104.

[85] R. Canetti, G. Even and O. Goldreich. Lower Bounds for Sampling Algorithms for Estimating the Average. *Information Processing Letters*, Vol. 53, pages 17–25, 1995.

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

[87] R. Canetti and R. Gennaro. Incoercible Multiparty Computation. In *37th IEEE Symposium on Foundations of Computer Science*, pages 504–513, 1996.

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

[89] R. Canetti, D. Micciancio and O. Reingold. Using one-way functions to construct Hash Functions that Hide All Partial Information. In *30th ACM Symposium on the Theory of Computing*, pages 131–140, 1998.

[90] R. Canetti, S. Halevi and A. Herzberg. How to Maintain Authenticated Communication in the Presence of Break-Ins. In *16th ACM Symposium on Principles of Distributed Computing*, pages 15–24, 1997.

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

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

[93] G.J. Chaitin. On the Length of Programs for Computing Finite Binary Sequences. *Journal of the ACM*, Vol. 13, pages 547–570, 1966.

[94] A.K. Chandra, D.C. Kozen and L.J. Stockmeyer. Alternation. *Journal of the ACM*, Vol. 28, pages 114–133, 1981.

[95] S. Chari, P. Rohatgi and A. Srinivasan. Improved Algorithms via Approximation of Probability Distributions. In *26th ACM Symposium on the Theory of Computing*, pages 584–592, 1994.

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

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

[98] D. Chaum, A. Fiat and M. Naor. Untraceable Electronic Cash. In *Crypto88*, Springer-Verlag Lecture Notes in Computer Science (Vol. 403), pages 319–327.

[99] R. Chang, B. Chor, O. Goldreich, J. Hartmanis, J. Håstad, D. Ranjan, and P. Rohatgi. The Random Oracle Hypothesis is False. *Journal of Computer and System Science*, Vol. 49, No. 1, pages 24–39, 1994.

[100] B. Chor and C. Dwork. Randomization in Byznatine Agreement. *Advances in Computing Research: A Research Annual*, Vol. 5 (Randomness and Computation, S. Micali, ed.), pages 443–497, 1989.

[101] B. Chor, J. Friedmann, O. Goldreich, J. Håstad, S. Rudich and R. Smolensky. The bit extraction problem and t-resilient functions. In *26th IEEE Symposium on Foundations of Computer Science*, pages 396–407, 1985.

[102] B. Chor and N. Gilboa. Computationally Private Information Retrieval. In *29th ACM Symposium on the Theory of Computing*, pages 304–313, 1997.

[103] B. Chor and O. Goldreich. On the Power of Two–Point Based Sampling. *Jour. of Complexity*, Vol 5, 1989, pages 96–106. Preliminary version dates 1985.

[104] B. Chor and O. Goldreich. Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity. *SIAM Journal on Computing*, Vol. 17, No. 2, pages 230–261, 1988.

[105] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, Private Information Retrieval. In *36th IEEE Symposium on Foundations of Computer Science*, pages 41–50, 1995.

[106] 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*, pages 383–395, 1985.

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

[108] A. Cohen and A. Wigderson. Dispensers, Deterministic Amplification, and Weak Random Sources. *30th IEEE Symposium on Foundations of Computer Science*, 1989, pages 14–19.

[109] T.M. Cover and G.A. Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc., New-York, 1991.

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

[111] R. Cramer and I. Damgård. Linear Zero-Knowledge – A Note on Efficient Zero-Knowledge Proofs and Arguments. In *29th ACM Symposium on the Theory of Computing*, pages 436–445, 1997.

[112] R. Cramer and I. Damgård. Zero-Knowledge Proofs for Finite Field Arithmetic; or: Can Zero-Knowledge be for Free? In *Crypto98*,

[113] R. Cramer, I. Damgård, and T. Pedersen. Efficient and provable security amplifications. In *Proc. of 4th Cambridge Security Protocols Workshop*, Springer, Lecture Notes in Computer Science (Vol. 1189), pages 101–109.

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

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

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

[117] I. Damgård, O. Goldreich, T. Okamoto and A. Wigderson. Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs. In *Crypto95*, Springer-Verlag Lecture Notes in Computer Science (Vol. 963), pages 325–338, 1995.

[118] A. De-Santis, Y. Desmedt, Y. Frankel and M. Yung. How to Share a Function Securely. In *26th ACM Symposium on the Theory of Computing*, pages 522–533, 1994.

[119] Y. Desmedt. Society and group oriented cryptography: A new concept. In *Crypto87*, Springer-Verlag, Lecture Notes in Computer Science (Vol. 293), pages 120–127.

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

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

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

[123] D. Dolev, M.J. Fischer, R. Fowler, N.A. Lynch and H.R. Strong. An efficient algorithm for Byzantine Agreement without authentication. *Information and Control*, Vol. 52(3), pages 257–274, March 1982.

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

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

[126] C. Dwork, U. Feige, J. Kilian, M. Naor and S. Safra. Low Communication Perfect Zero Knowledge Two Provers Proof Systems. In *Crypto92*, Springer Verlag, LNCS Vol. 740, pages 215–227, 1992.

[127] C. Dwork, and M. Naor. An Efficient Existentially Unforgeable Signature Scheme and its Application. To appear in *Journal of Cryptology*. Preliminary version in *Crypto94*.

[128] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Veličković. Approximations of General Independent Distributions. In *24th ACM Symposium on the Theory of Computing*, pages 10–16, 1992. Revised version available from `http://theory.lcs.mit.edu/~oded/papers.html`,

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

[130] S. Even, O. Goldreich, and A. Lempel. A Randomized Protocol for Signing Contracts. *Communications of the ACM*, Vol. 28, No. 6, 1985, pages 637–647.

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

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

[133] S. Even and Y. Yacobi. Cryptography and NP-Completeness. In proceedings of *7th ICALP*, Springer-Verlag Lecture Notes in Computer Science (Vol. 85), pages 195–207, 1980. See [132].

[134] U. Feige. A Threshold of ln n for Approximating Set Cover. In *28th ACM Symposium on the Theory of Computing*, pages 314–318, 1996.

[135] U. Feige. On the success probability of the two provers in One-Round Proof Systems. In *Proc. 6th IEEE Symp. on Structure in Complexity Theory*, pages 116–123, 1991.

[136] U. Feige. Error reduction by parallel repetition – the state of the art. Technical report CS95-32, Computer Science Department, Weizmann Institute of Science, Rehovot, ISREAL, 1995.

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

[138] U. Feige, S. Goldwasser, L. Lovász and S. Safra. On the Complexity of Approximating the Maximum Size of a Clique. Unpublished manuscript, 1990.

[139] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy. Approximating Clique is almost NP-complete. *Journal of the ACM*, Vol. 43, pages 268–292, 1996. Preliminary version in *32nd IEEE Symposium on Foundations of Computer Science*, 1991.

[140] U. Feige and J. Kilian. Two prover protocols – Low error at affordable rates. In *26th ACM Symposium on the Theory of Computing*, pages 172–183, 1994.

[141] U. Feige and J. Kilian. Zero knowledge and the chromatic number. In *11th IEEE Conference on Computational Complexity*, pages 278–287, 1996.

[142] U. Feige and J. Kilian. Making games short (extended abstract). In *29th ACM Symposium on the Theory of Computing*, pages 506–516, 1997.

[143] U. Feige, D. Lapidot, and A. Shamir. Multiple Non-Interactive Zero-Knowledge Proofs Based on a Single Random String. In *31th IEEE Symposium on Foundations of Computer Science*, pages 308–317, 1990. To appear in *SIAM Journal on Computing*.

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

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

[146] U. Feige, A. Shamir and M. Tennenholtz. The noisy oracle problem. In *Crypto88*, Springer-Verlag Lecture Notes in Computer Science (Vol. 403), pages 284–296.

[147] P. Feldman. A Practical Scheme for Non-interactive Verifiable Secret Sharing. In *28th IEEE Symposium on Foundations of Computer Science*, pages 427–437, 1987.

[148] P. Feldman and S. Micali. An optimal probabilistic protocol for synchronous Byzantine Agreement. *SICOMP*, Vol. 26, pages 873–933, 1997.

[149] A. Fiat. Batch RSA. *Journal of Cryptology*, Vol. 10, 1997, pages 75–88.

[150] 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), pages 186–189, 1987.

[151] J.B. Fischer and J. Stern. An Efficient Pseudorandom Generator Provably as Secure as Syndrome Decoding. In *EuroCrypt96*, Springer Lecture Notes in Computer Science (Vol. 1070), pages 245–255.

[152] R. Fischlin and C.P. Schnorr. Stronger Security Proofs for RSA and Rabin Bits. In *EuroCrypt97*, Springer Lecture Notes in Computer Science (Vol. 1233), pages 267–279, 1997.

[153] L. Fortnow, The Complexity of Perfect Zero-Knowledge. In *19th ACM Symposium on the Theory of Computing*, pages 204–209, 1987.

[154] L. Fortnow, J. Rompel and M. Sipser. On the power of multi-prover interactive protocols. In *Proc. 3rd IEEE Symp. on Structure in Complexity Theory*, pages 156–161, 1988.

[155] L. Fortnow, J. Rompel and M. Sipser. Errata for "On the power of multi-prover interactive protocols." In *Proc. 5th IEEE Symp. on Structure in Complexity Theory*, pages 318–319, 1990.

[156] M. Franklin and M. Yung. Secure and Efficient Off-Line Digital Money. In *20th ICALP*, Springer-Verlag Lecture Notes in Computer Science (Vol. 700), pages 265–276.

[157] 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, pages 262–280, 1988.

[158] M. Fürer, O. Goldreich, Y. Mansour, M. Sipser, and S. Zachos. On Completeness and Soundness in Interactive Proof Systems. *Advances in Computing Research: a research annual*, Vol. 5 (Randomness and Computation, S. Micali, ed.), pages 429–442, 1989.

[159] O. Gaber and Z. Galil. Explicit Constructions of Linear Size Superconcentrators. *Journal of Computer and System Science*, Vol. 22, pages 407–420, 1981.

[160] P.S. Gemmell. An Introduction to Threshold Cryptography. In *CryptoBytes*, RSA Lab., Vol. 2, No. 3, 1997.

[161] P. Gemmell, R. Lipton, R. Rubinfeld, M. Sudan, and A. Wigderson. Self-Testing/Correcting for Polynomials and for Approximate Functions. In *23th ACM Symposium on the Theory of Computing*, pages 32–42, 1991.

[162] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust Threshold DSS Signatures. In *EuroCrypt96*, Springer-Verlag, Lecture Notes in Computer Science (Vol. 1070), pages 354–371.

[163] M. Goemans and D. Williamson. New 3/4-approximation algorithms for the maximum satisfiablity problem. *SIAM Journal on Discrete Mathematics*, Vol. 7, No. 4, pages 656–666, 1994.

[164] M. Goemans and D. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM*, Vol. 42, No. 6, 1995, pages 1115–1145.

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

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

[167] O. Goldreich. *Lecture Notes on Encryption, Signatures and Cryptographic Protocol*. Spring 1989. Available from `http://theory.lcs.mit.edu/~oded/ln89.html`.

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

[169] O. Goldreich. Three XOR-Lemmas – An Exposition. *ECCC*, TR95-056, 1995. Available from `http://www.eccc.uni-trier.de/eccc/`.

[170] O. Goldreich. *Foundation of Cryptography – Fragments of a Book*. February 1995. Revised version, January 1998. Both versions are available from `http://theory.lcs.mit.edu/~oded/frag.html`.

[171] O. Goldreich. A Sample of Samplers – A Computational Perspective on Sampling. *ECCC*, TR97-020, May 1997.

[172] O. Goldreich. Notes on Levin's Theory of Average-Case Complexity. *ECCC*, TR97-058, Dec. 1997.

[173] O. Goldreich. *Secure Multi-Party Computation*. In preparation, 1998. Working draft available from `http://theory.lcs.mit.edu/~oded/gmw.html`.

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

[175] 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), pages 276–288, 1985.

[176] O. Goldreich and J. Håstad. On the Message Complexity of Interactive Proof Systems. To appear in *Information Processing Letters*. Available as TR96-018 of *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, 1996.

[177] O. Goldreich, R. Impagliazzo, L.A. Levin, R. Venkatesan, and D. Zuckerman. Security Preserving Amplification of Hardness. In *31st IEEE Symposium on Foundations of Computer Science*, pages 318–326, 1990.

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

[179] 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. Preliminary version in *17th ICALP*, 1990.

[180] O. Goldreich, and H. Krawczyk, On Sparse Pseudorandom Ensembles. *Random Structures and Algorithms*, Vol. 3, No. 2, (1992), pages 163–174.

[181] O. Goldreich, H. Krawcyzk and M. Luby. On the Existence of Pseudorandom Generators. *SIAM Journal on Computing*, Vol. 22-6, pages 1163–1175, 1993.

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

[183] O. Goldreich and B. Meyer. Computational Indistinguishability – Algorithms vs. Circuits. *Theoretical Computer Science*, Vol. 191, pages 215–218, 1998. Preliminary version by Meyer in *Structure in Complexity Theory*, 1994.

[184] O. Goldreich and S. Micali. Increasing the Expansion of Pseudorandom Generators. Manuscript, 1984. Available from `http://theory.lcs.mit.edu/~oded/papers.html`

[185] 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, pages 691–729, 1991. Preliminary version in *27th IEEE Symposium on Foundations of Computer Science*, 1986.

[186] 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,* pages 218–229, 1987.

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

[188] O. Goldreich and R. Ostrovsky. Software Protection and Simulation on Oblivious RAMs. *Journal of the ACM*, Vol. 43, 1996, pages 431–473.

[189] O. Goldreich and E. Petrank. Quantifying Knowledge Complexity. In *32nd IEEE Symposium on Foundations of Computer Science*, pp. 59–68, 1991.

[190] O. Goldreich, R. Rubinfeld and M. Sudan. Learning polynomials with queries: the highly noisy case. In *36th IEEE Symposium on Foundations of Computer Science*, pages 294–303, 1995.

[191] O. Goldreich and S. Safra. A Combinatorial Consistency Lemma with application to the PCP Theorem. In the proceedings of *Random97*, Springer Lecture Notes in Computer Science (Vol. 1269), pages 67–84. See also *ECCC*, TR96-047, 1996.

[192] O. Goldreich, A. Sahai, and S. Vadhan. Honest-Verifier Statistical Zero-Knowledge equals general Statistical Zero-Knowledge. In *30th ACM Symposium on the Theory of Computing*, pages 399–408, 1998.

[193] O. Goldreich and M. Sudan. Computational Indistinguishability: k versus $2k$ samples. In *13th IEEE Conference on Computational Complexity*, pages 24–33, 1998.

[194] O. Goldreich and A. Wigderson. Tiny Families of Functions with Random Properties: A Quality–Size Trade–off for Hashing. *Journal of Random structures and Algorithms*, Vol. 11, Nr. 4, December 1997, pages 315–343.

[195] O. Goldreich and D. Zuckerman. Another proof that BPP subseteq PH (and more). *ECCC*, TR97-045, 1997.

[196] S. Goldwasser. Fault Tolerant Multi Party Computations: Past and Present. In *16th ACM Symposium on Principles of Distributed Computing*, pages 1–6, 1997.

[197] 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), pages 77–93.

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

[199] S. Goldwasser, S. Micali and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, Vol. 18, pages 186–208, 1989. Preliminary version in *17th ACM Symposium on the Theory of Computing*, 1985. Earlier versions date to 1982.

[200] S. Goldwasser, S. Micali, and R.L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. *SIAM Journal on Computing*, April 1988, pages 281–308.

[201] 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.

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

[203] S. Goldwasser and M. Sipser. Private Coins versus Public Coins in Interactive Proof Systems. *Advances in Computing Research: a research annual*, Vol. 5 (Randomness and Computation, S. Micali, ed.), pages 73–90, 1989. Extended abstract in *18th ACM Symposium on the Theory of Computing*, pages 59–68, 1986.

[204] S. W. Golomb. *Shift Register Sequences*. Holden-Day, 1967. (Aegean Park Press, Revised edition, 1982.)

[205] V. Guruswami, D. Lewin, M. Sudan and L. Trevisan. A tight characterization of NP with 3 query PCPs. To appear in *39th IEEE Symposium on Foundations of Computer Science*, 1998.

[206] S. Hada and T. Tanaka. On the Existence of 3-Round Zero-Knowledge Protocols. In *Crypto98*,

[207] J. Håstad. Almost optimal lower bounds for small depth circuits. *Advances in Computing Research: a research annual*, Vol. 5 (Randomness and Computation, S. Micali, ed.), pages 143–170, 1989. Extended abstract in *18th ACM Symposium on the Theory of Computing*, pages 6–20, 1986.

[208] J. Håstad. Pseudo-Random Generators under Uniform Assumptions. In *22nd ACM Symposium on the Theory of Computing*, pages 395–404, 1990.

[209] J. Håstad. Clique is hard to approximate within $n^{1-\epsilon}$. To appear in *ACTA Mathematica*. Preliminary versions in *28th ACM Symposium on the Theory of Computing* (1996) and *37th IEEE Symposium on Foundations of Computer Science* (1996).

[210] J. Håstad. Getting optimal in-approximability results. In *29th ACM Symposium on the Theory of Computing*, pages 1–10, 1997.

[211] J. Håstad, R. Impagliazzo, L.A. Levin and M. Luby. Construction of Pseudorandom Generator from any One-Way Function. To appear in *SIAM Journal on Computing*. Combines the results of [217] and [208].

[212] J. Håstad, S. Phillips and S. Safra. A Well Characterized Approximation Problem. *Information Processing Letters*, Vol. 47:6, pages 301–305. 1993.

[213] J. Håstad, A. Schrift and A. Shamir. The Discrete Logarithm Modulo a Composite Hides $O(n)$ Bits. *Journal of Computer and System Science*, Vol. 47, pages 376–404, 1993.

[214] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk and M. Yung. Proactive public key and signature systems. In *1997 ACM Conference on Computers and Communication Security*, pages 100–110, 1997.

[215] A. Herzberg, S. Jarecki, H. Krawczyk and M. Yung. Proactive Secret Sharing, or How to Cope with Perpetual Leakage. In *Crypto95*, Springer-Verlag Lecture Notes in Computer Science (Vol. 963), pages 339–352.

[216] R. Impagliazzo. Hard-core Distributions for Somewhat Hard Problems. In *36th IEEE Symposium on Foundations of Computer Science*, pages 538–545, 1995.

[217] R. Impagliazzo, L.A. Levin and M. Luby. Pseudorandom Generation from One-Way Functions. In *21st ACM Symposium on the Theory of Computing*, pages 12–24, 1989.

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

[219] R. Impagliazzo and M. Naor. Efficient Cryptographic Schemes Provable as Secure as Subset Sum. *Journal of Cryptology*, Vol. 9, 1996, pages 199–216.

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

[221] R. Impagliazzo and A. Wigderson. P=BPP if E requires exponential circuits: Derandomizing the XOR Lemma. In *29th ACM Symposium on the Theory of Computing*, pages 220–229, 1997.

[222] R. Impagliazzo and M. Yung. Direct Zero-Knowledge Computations. In *Crypto87*, Springer-Verlag Lecture Notes in Computer Science (Vol. 293), pages 40–51, 1987.

[223] R. Impagliazzo and D. Zuckerman. How to Recycle Random Bits. In *30th IEEE Symposium on Foundations of Computer Science*, 1989, pages 248–253.

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

[225] J. Justesen. A class of constructive asymptotically good alegbraic codes. *IEEE Trans. Inform. Theory*, Vol. 18, pages 652–656, 1972.

[226] N. Kahale, Eigenvalues and Expansion of Regular Graphs. *Journal of the ACM*, 42(5):1091–1106, September 1995.

[227] D.R. Karger. Global Min-cuts in RNC, and Other Ramifications of a Simple Min-Cut Algorithm. In *4th SODA*, pages 21–30, 1993.

[228] H. Karloff and U. Zwick. A 7/8-approximation algorithm for MAX 3SAT? In *38th IEEE Symposium on Foundations of Computer Science*, 1997, pages 406–415.

[229] R.M. Karp and M. Luby. Monte-Carlo algorithms for enumeration and reliability problems. In *24th IEEE Symposium on Foundations of Computer Science*, pages 56-64, 1983. See [230].

[230] R.M. Karp, M. Luby and N. Madras. Monte-Carlo approximation algorithms for enumeration problems. *Journal of Algorithms*, Vol. 10, pages 429–448, 1989.

[231] R.M. Karp, N. Pippinger and M. Sipser. A Time-Randomness Tradeoff. *AMS Conference on Probabilistic Computational Complexity*, Durham, New Hampshire (1985).

[232] J. Kilian. A Note on Efficient Zero-Knowledge Proofs and Arguments. In *24th ACM Symposium on the Theory of Computing*, pages 723–732, 1992.

[233] J. Kilian and E. Petrank. An Efficient Non-Interactive Zero-Knowledge Proof System for NP with General Assumptions. *Journal of Cryptology*, Vol. 11, pages 1–27, 1998.

[234] D.E. Knuth. *The Art of Computer Programming*, Vol. 2 (*Seminumerical Algorithms*). Addison-Wesley Publishing Company, Inc., 1969 (first edition) and 1981 (second edition).

[235] A. Kolmogorov. Three Approaches to the Concept of "The Amount Of Information". *Probl. of Inform. Transm.*, Vol. 1/1, 1965.

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

[237] E. Kushilevitz and N. Nisan. *Communication Complexity*, Cambridge University Press, 1996.

[238] E. Kushilevitz and R. Ostrovsky. Replication is not Needed: A Single Database, Computational PIR. In *38th IEEE Symposium on Foundations of Computer Science*, pages 364–373, 1997.

[239] D. Lapidot and A. Shamir. Fully parallelized multi-prover protocols for NEXP-time. In *32nd IEEE Symposium on Foundations of Computer Science*, pages 13–18, 1991.

[240] C. Lautemann. BPP and the Polynomial Hierarchy. *Information Processing Letters*, 17, pages 215–217, 1983.

[241] F.T. Leighton. *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes*. Morgan Kaufmann Publishers, San Mateo, CA, 1992.

[242] A. Lempel. Cryptography in Transition. *Computing Surveys*, Dec. 1979.

[243] L.A. Levin. Randomness Conservation Inequalities: Information and Independence in Mathematical Theories. *Inform. and Control*, Vol. 61, pages 15–37, 1984.

[244] L.A. Levin. Average Case Complete Problems. *SIAM Jour. of Computing*, Vol. 15, pages 285–286, 1986.

[245] L.A. Levin. One-Way Function and Pseudorandom Generators. *Combinatorica*, Vol. 7, pages 357–363, 1987.

[246] M. Li and P. Vitanyi. *An Introduction to Kolmogorov Complexity and its Applications*. Springer Verlag, August 1993.

[247] N. Linial, M. Luby, M. Saks and D. Zuckerman. Efficient construction of a small hitting set for combinatorial rectangles in high dimension. In *25th ACM Symposium on the Theory of Computing*, pages 258–267, 1993.

[248] R.J. Lipton. New Directions in Testing. In *Proc. of DIMACS Workshop on Distr. Comp. and Crypto.*, pages 191–202, 1991.

[249] A. Lubotzky, R. Phillips, P. Sarnak, Ramanujan Graphs. *Combinatorica*, Vol. 8, pages 261–277, 1988.

[250] M. Luby. A Simple Parallel Algorithm for the Maximal Independent Set Problem. *SIAM Journal on Computing*, Vol. 15, No. 4, pages 1036–1053, November 1986. Preliminary version in *17th ACM Symposium on the Theory of Computing*, 1985.

[251] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton University Press, 1996.

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

[253] M. Luby, B. Veličković and A. Wigderson. Deterministic Approximate Counting of Depth-2 Circuits. In *2nd Israel Symp. on Theory of Computing and Systems (ISTCS93)*, IEEE Computer Society Press, pages 18–24, 1993.

[254] M. Luby and A. Wigderson. Pairwise Independence and Derandomization. TR-95-035, International Computer Science Institute (ICSI), Berkeley, 1995. ISSN 1075-4946.

[255] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic Methods for Interactive Proof Systems. *Journal of the ACM*, Vol. 39, No. 4, pages 859–868, 1992. Preliminary version in *31st IEEE Symposium on Foundations of Computer Science*, 1990.

[256] C. Lund and M. Yannakakis. On the Hardness of Approximating Minimization Problems, In *25th ACM Symposium on the Theory of Computing*, pages 286–293, 1993.

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

[258] G.A. Margulis. Explicit Construction of Concentrators. *Prob. Per. Infor.* 9 (4) (1973), 71–80. (In Russian, English translation in *Problems of Infor. Trans.* (1975), 325–332.)

[259] U. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. on Inform. Th.* , Vol. 39 (No. 3), pages 733–742, May 1993.

[260] R.C. Merkle. Secure Communication over Insecure Channels. *Communications of the ACM*, Vol. 21, No. 4, pages 294–299, 1978.

[261] R.C. Merkle. Protocols for public key cryptosystems. In *Proc. of the 1980 Symposium on Security and Privacy.*

[262] 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.

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

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

[265] S. Micali. Fair Public-Key Cryptosystems. In *Crypto92*, Springer-Verlag Lecture Notes in Computer Science (Vol. 740), pages 113–138.

[266] S. Micali. CS Proofs. Unpublished manuscript, 1992.

[267] S. Micali. CS Proofs. In *35th IEEE Symposium on Foundations of Computer Science*, pages 436–453, 1994. A better version is available from the author.

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

[269] R. Motwani and P. Raghavan. *Randomized Algorithms*, Cambridge University Press, 1995.

[270] K. Mulmuley and U.V. Vazirani and V.V. Vazirani. Matching is as Easy as Matrix inversion. *Combinatorica*, Vol. 7, pages 105–113, 1987.

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

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

[273] M. Naor, L.J. Schulman and A. Srinivasan. Splitters and near-optimal derandomization. In *36th IEEE Symposium on Foundations of Computer Science*, pages 182-191, 1995.

[274] J. Naor and M. Naor. Small-bias Probability Spaces: Efficient Constructions and Applications. *SIAM J. on Computing*, Vol 22, 1993, pages 838–856.

[275] M. Naor, R. Ostrovsky, R. Venkatesan and M. Yung. Zero-Knowledge Arguments for NP can be Based on General Assumptions. In *Crypto92*, Springer-Verlag Lecture Notes in Computer Science (Vol. 740), pages 196–214.

[276] M. Naor and O. Reingold. Synthesizers and their Application to the Parallel Construction of Pseudo-Random Functions. In *36th IEEE Symposium on Foundations of Computer Science*, pages 170–181, 1995.

[277] M. Naor and O. Reingold. On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited. In *29th ACM Symposium on the Theory of Computing*, pages 189–199, 1997.

[278] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudorandom functions and other cryptographic primitives. In *38th IEEE Symposium on Foundations of Computer Science*, pages 458–467, 1997.

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

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

[281] N. Nisan. Pseudorandom bits for constant depth circuits. *Combinatorica*, Vol. 11 (1), pages 63–70, 1991.

[282] N. Nisan. Pseudorandom Generators for Space Bounded Computation. *Combinatorica*, Vol. 12 (4), pages 449–461, 1992.

[283] N. Nisan. $\mathcal{RL} \subseteq \mathcal{SC}$. *Journal of Computational Complexity*, Vol. 4, pages 1-11, 1994.

[284] N. Nisan. Extracting Randomness: How and Why – A Survey. In *11th IEEE Conference on Computational Complexity*, pages 44–58, 1996.

[285] N. Nisan, E. Szemeredi, and A. Wigderson. Undirected connectivity in $O(log^{1.5}n)$ space. In *33rd IEEE Symposium on Foundations of Computer Science*, pages 24-29, 1992.

[286] N. Nisan and A. Wigderson. Hardness vs Randomness. *Journal of Computer and System Science*, Vol. 49, No. 2, pages 149–167, 1994.

[287] N. Nisan and D. Zuckerman. Randomness is Linear in Space. To appear in *Journal of Computer and System Science*. Preliminary version in *25th ACM Symposium on the Theory of Computing*, pages 235–244, 1993.

[288] A.M. Odlyzko. The future of integer factorization. *CryptoBytes* (The technical newsletter of RSA Laboratories), Vol. 1 (No. 2), pages 5-12, 1995. Available from `http://www.research.att.com/~amo`

[289] A.M. Odlyzko. Discrete logarithms and smooth polynomials. In *Finite Fields: Theory, Applications and Algorithms*, G. L. Mullen and P. Shiue, eds., Amer. Math. Soc., Contemporary Math. Vol. 168, pages 269–278, 1994. Available from `http://www.research.att.com/~amo`

[290] T. Okamoto. On relationships between statistical zero-knowledge proofs. In *28th ACM Symposium on the Theory of Computing*, pages 649–658, 1996.

[291] M. Ogihara. Sparse P-hard sets yield space-efficient algorithms. In *36th IEEE Symposium on Foundations of Computer Science*, pages 354–361, 1995.

[292] R. Ostrovsky and A. Wigderson. One-Way Functions are essential for Non-Trivial Zero-Knowledge. In *2nd Israel Symp. on Theory of Computing and Systems*, IEEE Comp. Soc. Press, pages 3–17, 1993.

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

[294] C. H. Papadimitriou and M. Yannakakis. Optimization, Approximation, and Complexity Classes. In *20th ACM Symposium on the Theory of Computing*, pages 229–234, 1988.

[295] M. Pease, R. Shostak and L. Lamport. Reaching agreement in the presence of faults. *Journal of the ACM*, Vol. 27(2), pages 228–234, 1980.

[296] T.P. Pedersen and B. Pfitzmann. Fail-Stop Signatures. *SIAM Journal on Computing*, Vol. 26/2, pages 291–330, 1997. Based on several earlier work (see first footnote in the paper).

[297] E. Petrank and G. Tardos. On the Knowledge Complexity of NP. In *37th IEEE Symposium on Foundations of Computer Science*, pages 494–503, 1996.

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

[299] B. Pfitzmann and M. Waidner. How to break and repair a "provably secure" untraceable payment system. In *Crypto91*, Springer-Verlag Lecture Notes in Computer Science (Vol. 576), pages 338–350.

[300] B. Pfitzmann and M. Waidner. Properties of Payment Systems: General Definition Sketch and Classification. IBM Research Report RZ2823 (#90126), IBM Research Division, Zurich, May 1996.

[301] A. Polishchuk and D.A. Spielman. Nearly-linear size holographic proofs. In *26th ACM Symposium on the Theory of Computing*, pages 194–203, 1994.

[302] M.O. Rabin. Digitalized Signatures. In *Foundations of Secure Computation* (R.A. DeMillo et. al. eds.), Academic Press, 1977.

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

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

[305] M.O. Rabin. Randomized Byznatine Agreement. In *24th IEEE Symposium on Foundations of Computer Science*, pages 403–409, 1983.

[306] 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*, pages 73–85, 1989.

[307] 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), pages 433–444.

[308] P. Raghavan and C.D. Thompson. Randomized Rounding. *Combinatorica*, Vol. 7, pages 365–374, 1987.

[309] R. Raz. A Parallel Repetition Theorem. In *27th ACM Symposium on the Theory of Computing*, pages 447–456, 1995.

[310] R. Raz and S. Safra. A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP. In *29th ACM Symposium on the Theory of Computing*, pages 475–484, 1997.

[311] A.R. Razborov and S. Rudich. Natural proofs. *Journal of Computer and System Science*, Vol. 55 (1), pages 24–35, 1997.

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

[313] 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.

[314] R. Rubinfeld and M. Sudan. Robust Characterizations of Polynomials with Applications to Program Checking. *SIAM J. of Computing*, Vol. 25, No. 2, pages 252–271, 1996. Preliminary version in *3rd SODA*, 1992.

[315] S. Rudich. Super-bits, Demi-bits, and $\widetilde{\mathrm{NP}}$/qpoly-Natural proofs. In the proceedings of *Random97*, Springer Lecture Notes in Computer Science (Vol. 1269), pages 85–93.

[316] A. Sahai and S. Vadhan. A Complete Promise Problem for Statistical Zero-Knowledge. In *38th IEEE Symposium on Foundations of Computer Science*, pages 448–457, 1997.

[317] M. Saks. Randomization and derandomization in space-bounbded computation. In *11th IEEE Conference on Computational Complexity*, pages 128–149, 1996.

[318] M. Saks, A. Srinivasan and S. Zhou. Explicit dispersers with polylog degree. In *27th ACM Symposium on the Theory of Computing*, pages 479–488, 1995.

[319] M. Saks and S. Zhou. $RSPACE(S) \subseteq DSPACE(S^{3/2})$. In 36th *IEEE Symposium on Foundations of Computer Science*, pages 344–353, 1995.

[320] C.P. Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, Vol. 4, pages 161–174, 1991.

[321] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, Vol. 27, pages 701–717, 1980.

[322] C.E. Shannon. A mathematical theory of communication. *Bell Sys. Tech. Jour.*, Vol. 27, pages 623–656, 1948.

[323] C.E. Shannon. Communication Theory of Secrecy Systems. *Bell Sys. Tech. Jour.*, Vol. 28, pages 656–715, 1949.

[324] A. Shamir. How to Share a Secret. *Communications of the ACM*, Vol. 22, Nov. 1979, pages 612–613.

[325] A. Shamir. IP = PSPACE. *Journal of the ACM*, Vol. 39, No. 4, pages 869–877, 1992. Preliminary version in *31st IEEE Symposium on Foundations of Computer Science*, 1990.

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

[327] A. Shen. IP = PSPACE: Simplified proof. *Journal of the ACM*, Vol. 39, No. 4, pages 878–880, 1992.

[328] D. Simon. Anonymous Communication and Anonymous Cash. In *Crypto96*, Springer Lecture Notes in Computer Science (Vol. 1109), pages 61–73.

[329] M. Sipser. A Complexity Theoretic Approach to Randomness. In *15th ACM Symposium on the Theory of Computing*, pages 330–335, 1983.

[330] M. Sipser. Private communication, 1986.

[331] M. Sipser. Expanders, randomness, or time versus space. *Journal of Computer and System Science*, Vol. 36(3), pages 379–383, 1988. Preliminary version in *Structure in Complexity Theory*, 1986.

[332] M. Sipser. *Introduction to the Theory of Computation*, PWS Publishing Company, 1997.

[333] R.J. Solomonoff. A Formal Theory of Inductive Inference. *Inform. and Control*, Vol. 7/1, pages 1–22, 1964.

[334] L. Stockmeyer. The Complexity of Approximate Counting. In *15th ACM Symposium on the Theory of Computing*, pages 118–126, 1983.

[335] M. Sudan and L. Trevisan. Probabilistic Checkable Proofs with Low Amortized Query Complexity. To appear in *39th IEEE Symposium on Foundations of Computer Science*, 1998.

[336] A. Ta-Shma. Note on PCP vs. MIP. *Information Processing Letters*, Vol. 58, No. 3, pages 135–140, 1996.

[337] A. Ta-Shma. On extracting randomness from weak random sources. In *28th ACM Symposium on the Theory of Computing*, pages 276-285, 1996.

[338] S. Toueg, K.J. Perry and T.K. Srikanth. Fast distributed agreement. *SIAM Journal on Computing*, Vol. 16(3), pages 445–457, 1987.

[339] L. Trevisan. Private communication, 1997. See [171, Sec. 5.2].

[340] L. Trevisan. When Hamming meets Euclid: The Approximability of Geometric TSP and MST. In *29th ACM Symposium on the Theory of Computing*, pages 21–29, 1997.

[341] L.G. Valiant. A scheme for fast parallel communication. *SIAM Journal on Computing*, Vol. 11 (2), pages 350–361, 1982.

[342] L.G. Valiant. A theory of the learnable. *Communications of the ACM*, Vol. 27/11, pages 1134–1142, 1984.

[343] L.G. Valiant and G.J. Brebner. Universal schemes for parallel communication. In *13th ACM Symposium on the Theory of Computing*, pages 263–277, 1981.

[344] L.G. Valiant and V.V. Vazirani. NP Is as Easy as Detecting Unique Solutions. *Theoretical Computer Science*, Vol. 47 (1), pages 85–93, 1986.

[345] U.V. Vazirani. Randomness, Adversaries and Computation. Ph.D. Thesis, EECS, UC Berkeley, 1986.

[346] U.V. Vazirani and V.V. Vazirani. Efficient and Secure Pseudo-Random Number Generation. In *25th IEEE Symposium on Foundations of Computer Science*, pages 458–463, 1984.

[347] U.V. Vazirani and V.V. Vazirani. Random Polynomial Time Equal to Semi-Random Polynomial Time. In *26th IEEE Symposium on Foundations of Computer Science*, pages 417–428, 1985.

[348] 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.

[349] A. Wigderson. The amazing power of pairwise independence. In *26th ACM Symposium on the Theory of Computing*, pages 645–647, 1994.

[350] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, Vol. 54 (No. 8), pages 1355–1387, Oct. 1975.

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

[352] A.C. Yao. Separating the polynomial-time hierarchy by oracles. In *26th IEEE Symposium on Foundations of Computer Science*, pages 1-10, 1985.

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

[354] R. Zippel. Probabilistic algorithms for sparse polynomials. *Proc. Int'l. Symp. on Symbolic and Algebraic Computation*, Springer-Verlag Lecture Notes in Computer Science (Vol. 72), pages 216–226, 1979.

[355] D. Zuckerman. Simulating BPP Using a General Weak Random Source. *Algorithmica*, Vol. 16, pages 367–391, 1996.

[356] D. Zuckerman. Randomness-Optimal Oblivious Sampling. *Journal of Random structures and Algorithms*, Vol. 11, Nr. 4, December 1997, pages 345–367.

[357] U. Zwick. Approximation algorithms for constraint satisfaction problems involving at most three variables per constraint. In *9th SODA*, 1998, pages 201–210.