List of Publications

Oded Goldreich

July 1, 2002

Contents

1 Theses

- On the Complexity of Some Edge Testing Problems, M.Sc. thesis, Computer Science Department, Technion, Haifa, Israel.

  Thesis adviser: Prof. S. Even, 1982.

- On the Security of Cryptographic Protocols and Cryptosystems, D.Sc. thesis, Computer Science Department, Technion, Haifa, Israel.

  Thesis adviser: Prof. S. Even, 1983.

2 Original Papers in Refereed Journals

Published

[J1] S. Even and O. Goldreich, The Minimum Length Generator Sequence is NP-Hard, *Journal of Algorithms*, vol. 2, pp. 311–313, 1981.

[J2] S. Even and O. Goldreich, DES-Like Functions Can Generate the Alternating Group, *IEEE Trans. on Inform. Theory*, Vol. IT-29, No. 6, pp. 863–865, 1983.

[J3] S. Even, O. Goldreich, S. Moran and P. Tong, On the NP-Completeness of Certain Network-Testing Problems, *Networks*, Vol. 14, No. 1, pp. 1–24, 1984.

[J4] S. Even, O. Goldreich, and A. Lempel, A Randomized Protocol for Signing Contracts, *Comm. of the ACM*, Vol. 28, No. 6, pp. 637–647, 1985.

[J5] S. Even and O. Goldreich, On the Power of Cascade Ciphers, *ACM Trans. on Computer Systems*, Vol. 3, No. 2, pp. 108–116, 1985.

[J6] O. Goldreich, S. Goldwasser and S. Micali, How to Construct Random Functions, *Jour. of the ACM*, Vol. 33, No. 4, Oct. 1986, pp. 792–807.

[J7] O. Goldreich and L. Shrira, Electing a Leader in a Ring with Link Failures, *ACTA Informatica*, 24, pp. 79–91, 1987.

[J8] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, RSA/Rabin Functions: Certain Parts are As Hard As the Whole, *SIAM J. Comp.*, Vol. 17, No. 2, April 1988, pp. 194–209.

[J9] B. Chor and O. Goldreich, Unbiased Bits From Sources of Weak Randomness and Probabilistic Communication Complexity, *SIAM J. Comp.*, Vol. 17, No. 2, April 1988, pp. 230–261.

[J10] B. Chor and O. Goldreich, On the Power of Two–Point Based Sampling, *Jour. of Complexity*, Vol 5, 1989, pp. 96–106.

[J11] M. Furer, 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.), pp. 429–442, 1989.

[J12] B. Chor and O. Goldreich, An Improved Parallel Algorithm for Integer GCD, *Algorithmica*, 5, pp. 1–10, 1990.

[J13] M. Ben-Or, O. Goldreich, S. Micali and R.L. Rivest, A Fair Protocol for Signing Contracts, *IEEE Trans. on Inform. Theory*, Vol. 36, No. 1, pp. 40–46, Jan. 1990.

[J14] O. Goldreich, On the Number of Monochromatic and Close Beads in a Rosary, *Discrete Mathematics*, Vol. 80, 1990, pp. 59–68.

[J15] B. Awerbuch, O. Goldreich, D. Peleg, and R. Vainish, A Trade-off between Information and Communication in Broadcast Protocols, *Jour. of the ACM*, Vol. 37, No. 2, April 1990, pp. 238–256.

[J16] O. Goldreich, A Note on Computational Indistinguishability, *IPL*, Vol. 34, pp. 277–281, May 1990.

[J17] O. Goldreich, and E. Petrank, The Best of Both Worlds: Guaranteeing Termination in Fast Randomized Byzantine Agreement Protocols, *IPL*, Vol. 36, October 1990, pp. 45–49.

[J18] O. Goldreich, S. Micali, and A. Wigderson, Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs, *Jour. of the ACM*, Vol. 38, No. 3, July 1991, pp. 691–729.

[J19] R. Bar-Yehuda, O. Goldreich, and A. Itai, Efficient Emulation of Single-Hop Radio Network with Collision Detection on Multi-Hop Radio Network with no Collision Detection, *Distributed Computing*, Vol. 5, 1991, pp. 67–71.

[J20] O. Goldreich and L. Shrira, On the Complexity of Global Computation in the Presence of Link Failures : The Case of a Ring, *Distributed Computing*, Vol. 5, 1991, pp. 121–131.

[J21] S. Ben-David, B. Chor, O. Goldreich, and M. Luby, On the Theory of Average Case Complexity, *Journal of Computer and system Sciences*, Vol. 44, No. 2, April 1992, pp. 193–219.

[J22] O. Goldreich, and H. Krawczyk, On Sparse Pseudorandom Ensembles, *Random Structures and Algorithms*, Vol. 3, No. 2, (1992), pp. 163–174.

[J23] N. Alon, O. Goldreich, J. Hastad, R. Peralta, Simple Constructions of Almost k-wise Independent Random Variables, *Journal of Random structures and Algorithms*, Vol. 3, No. 3, (1992), pp. 289–304.

[J24] R. Bar-Yehuda, O. Goldreich, A. Itai, On the Time-Complexity of Broadcast in Radio Networks: An Exponential Gap Between Determinism and Randomization, *Journal of Computer and system Sciences*, Vol. 45, (1992), pp. 104–126.

[J25] O. Goldreich, A Uniform Complexity Treatment of Encryption and Zero-Knowledge, *Journal of Cryptology*, Vol. 6, No. 1, (1993), pp. 21–53.

[J26] O. Goldreich and E. Kushilevitz, A Perfect Zero-Knowledge Proof for a Decision Problem Equivalent to Discrete Logarithm, *Journal of Cryptology*, Vol. 6, No. 2, (1993), pp. 97–116.

[J27] R. Canetti, and O. Goldreich, Bounds on Tradeoffs between Randomness and Communication Complexity, *Computational Complexity*, Vol. 3 (1993), pp. 141–167.

[J28] O. Goldreich, H. Krawczyk, and M. Luby, On the Existence of Pseudorandom Generators, *SIAM J. on Computing*, Vol. 22-6 (Dec. 1993), pp. 1163–1175.

[J29] M. Bellare, O. Goldreich, and S. Goldwasser, Randomness in Interactive Proofs, *Computational Complexity*, Vol. 4, No. 4 (1993), pp. 319–354.

[J30] O. Goldreich and Y. Oren, Definitions and Properties of Zero-Knowledge Proof Systems, *Journal of Cryptology*, Vol. 7, No. 1 (1994), pp. 1–32.

[J31] R. Chang, B. Chor, O. Goldreich, J. Hartmanis, J. Hastad, D. Ranjan and P. Rohatgi, The Random Oracle Hypothesis is False, *JCSS*, Vol. 49, No. 1 (1994), pp. 24–39.

[J32] R. Canetti, G. Even, and O. Goldreich, Lower Bounds for Sampling Algorithms for Estimating the Average, *IPL*, Vol. 53, pp. 17–25, 1995.

[J33] O. Goldreich, and H. Krawczyk, On the Composition of Zero-Knowledge Proof Systems, *SIAM Journal on Computing*, Vol. 25, No. 1, February 1996, pp. 169–192.

[J34] S. Even, O. Goldreich, and S. Micali, On-line/Off-line Digital signatures, *Journal of Cryptology*, Vol. 9, No. 1, 1996, pp. 35–67.

[J35] O. Goldreich, and R. Ostrovsky, Software Protection and Simulation on Oblivious RAMs, *JACM*, Vol. 43, No. 3, 1996, pp. 431–473.

[J36] O. Goldreich and A. Kahan, How to Construct Constant-Round Zero-Knowledge Proof Systems for NP, *Journal of Cryptology*, Vol. 9, No. 2, 1996, pp. 167–189.

[J37] O. Goldreich and D. Ron, On Universal Learning Algorithms, *IPL*, Vol. 63, 1997, pages 131–136.

[J38] 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*, Volume 11, Number 4, December 1997, pages 315–343.

[J39] O. Goldreich and B. Meyer, Computational Indistinguishability – Algorithms vs. Circuits, *Theoretical Computer Science*, Vol. 191 (1998), pages 215–218.

[J40] O. Goldreich, S. Goldwasser, and N. Linial, Fault-tolerant Computations without Assumptions: the Two-party Case, *SIAM J. on Computing*, Volume 27, Number 2, April 1998, Pages 506–544.

[J41] M. Bellare, O. Goldreich and M. Sudan, Free Bits, PCPs and Non-Approximability – Towards Tight Results, *SICOMP*, Vol. 27, No. 3, pp. 804–915, June 1998.

[J42] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Veličković, Efficient Approximations of Product Distributions, *Random Structures and Algorithms*, Vol. 13, No. 1, pp. 1–16, Aug. 1998.

[J43] O. Goldreich and J. Hastad, On the Complexity of Interactive Proofs with Bounded Communication, *IPL*, Vol. 67 (4), pages 205–214, 1998.

[J44] O. Goldreich, S. Goldwasser and D. Ron, Property Testing and its connection to Learning and Approximation, *Journal of the ACM*, pages 653–750, July 1998.

[J45] O. Goldreich, R. Ostrovsky and E. Petrank, Knowledge Complexity and Computational Complexity, *SICOMP*, Volume 27, Number 4, pp. 1116–1141, August 1998.

[J46] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, Private Information Retrieval, *Journal of the ACM*, Vol. 45, No. 6, pages 965–982, November 1998.

[J47] A. De Santis, G. Di Crescenzo, O. Goldreich, and G. Persiano, The Graph Clustering Problem has a Perfect Zero-Knowledge Proof, *IPL*, Vol. 69, pp. 201–206, 1999.

[J48] O. Goldreich and E. Petrank, Quantifying Knowledge Complexity, *Computational Complexity*, Vol. 8, pages 50–98, 1999.

[J49] O. Goldreich and D. Ron, A Sublinear Bipartitness Tester for Bounded Degree Graphs, *Combinatorica*, Vol. 19 (3), pages 335–373, 1999.

[J50] O. Goldreich, D. Micciancio, S. Safra, and J.P. Seifert, Approximating shortest lattice vectors is not harder than approximating closest lattice vectors, *IPL*, 71, pages 55–61, 1999.

[J51] O. Goldreich and M. Sudan, Computational Indistinguishability: A Sample Hierarchy, *JCSS*, Vol. 59, pages 253–269, 1999.

[J52] S. Decatur, O. Goldreich, and D. Ron, Computational Sample Complexity, *SICOMP*, Vol. 29, Nr. 3, pages 854–879, 1999.

[J53] O. Goldreich and S. Safra, A Combinatorial Consistency Lemma with application to the PCP Theorem, *SICOMP*, Volume 29, Number 4, pages 1132–1154, 1999.

[J54] O. Goldreich and S. Goldwasser, On the Limits of Non-Approximability of Lattice Problems, *JCSS*, Vol. 60, pages 540–563, 2000.

[J55] O. Goldreich, D. Ron and M. Sudan, Chinese Remaindering with Errors, *IEEE Transactions on Information Theory*, Vol. 46, No. 4, July 2000, pages 1330–1338.

[J56] O. Goldreich, S. Goldwasser, E. Lehman, D. Ron, and A. Samorodnitsky, Testing Monotinicity, *Combinatorica*, Vol. 20 (3), pages 301–337, 2000.

[J57] O. Goldreich, R. Rubinfeld and M. Sudan, Learning polynomials with queries: the highly noisy case, *SIAM J. on Disc. Math.*, Vol. 13, No. 4, pages 535–570, 2000.

[J58] M. Bellare, O. Goldreich and E. Petrank. Uniform Generation of NP-witnesses using an NP-oracle, *Inform. and Comp.*, Vol. 163, pages 510–526, 2000.

[J59] O. Goldreich and D. Ron. Property Testing in Bounded Degree Graphs, *Algorithmica*, 32 (2), pages 302–343, 2002.

Accepted

[J60] O. Goldreich and V. Rosen, On the Security of Modular Exponentiation with Application to the Construction of Pseudorandom Generators, *Jour. of Cryptology*, May 2001.

Submitted

[J61] R. Canetti, O. Goldreich and S. Halevi, The Random Oracle Methodology, Revisited, *Jour. of the ACM*, October 2000

[J62] O. Goldreich and Y. Lindell, Session-Key Generation using Human Passwords Only, *Jour. of the ACM*, Dec. 2001

[J63] O. Goldreich and L. Trevisan, Three Theorems regarding Testing Graph Properties, *Random Structures and Algorithms*, Dec. 2001

[J64] O. Goldreich, S. Vadhan and A. Wigderson, On interactive proofs with a laconic provers, *Computational Complexity*, May 2002

3 Original Papers in (Refereed) Conference Proceedings

General Theory of Computation Conferences (e.g. FOCS, STOC)

[C1] S. Even and O. Goldreich, On The Security of Multi-Party Ping-Pong Protocols, *Proc. of the 24th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 34-39, 1983.

[C2] W. Alexi, B. Chor, O. Goldreich, and C.P. Schnorr, RSA/Rabin Bits Are $1/2 + 1/poly(logN)$-Secure, *Proc. of the 25th IEEE Symp. on Foundation of Computer Science (FOCS)*, 1984, pp. 449-457. (This is an extended abstract of No. J8.)

[C3] O. Goldreich, S. Goldwasser and S. Micali, How to Construct Random Functions, *Proc. of the 25th IEEE Symp. on Foundation of Computer Science (FOCS)*, 1984, pp. 464-479. (This is an extended abstract of No. J6.)

[C4] M. Ben-Or, O. Goldreich, S. Micali and R.L. Rivest, A Fair Protocol for Signing Contracts, *Proc. of the 12th International Colloquium on Automata Languages and Programming (ICALP)*, Lecture Note in Computer Science (194) Springer Verlag, 1985, pp. 43-52. (This is an extended abstract of No. J13.)

[C5] B. Chor, J. Friedmann, O. Goldreich, J. Hastad, S. Rudich and R. Smolansky, The Bit Extraction Problem or t-Resilient Functions, *Proc. of the 26th IEEE Symp. on Foundation of Computer Science (FOCS)*, 1985, pp. 396-407.

[C6] B. Chor and O. Goldreich, Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity, *Proc. of the 26th IEEE Symp. on Foundation of Computer Science (FOCS)*, 1985, pp. 429-442. (This is an extended abstract of No. J9.)

[C7] O. Goldreich, S. Micali, and A. Wigderson, Proofs that Yield Nothing but their Validity and a Methodology of Cryptographic Protocol Design, *Proc. of the 27th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 174-187, 1986. (This is an extended abstract of No. J18.)

[C8] O. Goldreich, Towards a Theory of Software Protection and Simulation by Oblivious RAMs, *Proc. of the 19th ACM Symp. on Theory of Computing (STOC)*, pp. 182-194, 1987. (This extended abstract has been merged with an improvement by Rafail Ostrovsky to yield No. J35.)

[C9] O. Goldreich, S. Micali, and A. Wigderson, How to Play any Mental Game or a Completeness Theorem for Protocols with Honest Majority, *Proc. of the 19th ACM Symp. on Theory of Computing (STOC)*, pp. 218-229, 1987.

[C10] O. Goldreich, Y. Mansour, and M. Sipser, Interactive Proof Systems: Provers that never Fail and Random Selection, *Proc. of the 28th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 449-461, 1987. (This is a preliminary version of No. J11.)

[C11] O. Goldreich, H. Krawczyk, and M. Luby, On the Existence of Pseudorandom Generators, *Proc. of the 29th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 12-24, 1988. (This is an extended abstract of No. J28.)

[C12] O. Goldreich, and L.A. Levin, Hard-core Predicates for any One-Way Function, *Proc. of the 21st ACM Symp. on Theory of Computing (STOC)*, pp. 25-32, 1989.

[C13] S. Ben-David, B. Chor, O. Goldreich, and M. Luby, On the Theory of Average Case Complexity, *Proc. of the 21st ACM Symp. on Theory of Computing (STOC)*, pp. 204-216, 1989. (This is an extended abstract of No. J21.)

[C14] O. Goldreich, and H. Krawczyk, On the Composition of Zero-Knowledge Proof Systems, *Proc. of the 17th International Colloquium on Automata Languages and Programming (ICALP)*, Lecture Notes in Computer Science, Vol. 443, Springer Verlag, pp. 268–282, 1990. (This is an extended abstract of No. J33.)

[C15] O. Goldreich, R. Impagliazzo, L.A. Levin, R. Venkatesan, and D. Zuckerman, Security Preserving Amplification of Hardness, *Proc. of the 31st IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 318–326, 1990.

[C16] N. Alon, O. Goldreich, J. Hastad, R. Peralta, Simple Constructions of Almost k-wise Independent Random Variables, *Proc. of the 31st IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 544–553, 1990. (This is an extended abstract of No. J23.)

[C17] M. Bellare, O. Goldreich, and S. Goldwasser, Randomness in Interactive Proofs, *Proc. of the 31st IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 563–572, 1990. (This is an extended abstract of No. J29.)

[C18] R. Canetti, and O. Goldreich, Bounds on Tradeoffs between Randomness and Communication Complexity, *Proc. of the 31st IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 766–775, 1990. (This is an extended abstract of No. J27.)

[C19] O. Goldreich, S. Goldwasser, and N. Linial, Fault-tolerant Computations without Assumptions: the Two-party Case, *Proc. of the 32nd IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 447–457, 1991. (This is an extended abstract of No. J40.)

[C20] O. Goldreich, and E. Petrank, Quantifying Knowledge Complexity, *Proc. of the 32nd IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 59–68, 1991. (This is an extended abstract of No. J48.)

[C21] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Veličković, Approximations of General Independent Distributions, *Proc. of the 24th ACM Symp. on Theory of Computing (STOC)*, pp. 10–16, 1992. (This is an extended abstract of No. J42.)

[C22] M. Blum and O. Goldreich, Towards a Computational Theory of Statistical Tests, *Proc. of the 33rd IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 406-416, 1992.

[C23] M. Ben-Or, R. Canetti and O. Goldreich, Asynchronous Secure Computation, *Proc. of the 25th ACM Symp. on Theory of Computing (STOC)*, pp. 52-61, 1993.

[C24] O. Goldreich and A. Wigderson, Tiny Families of Functions with Random Properties: A Quality–Size Trade–off for Hashing, *Proc. of the 26th ACM Symp. on Theory of Computing (STOC)*, pp. 574-583, 1994. (This is an extended abstract of No. J38.)

[C25] O. Goldreich, R. Ostrovsky and E. Petrank, Knowledge Complexity and Computational Complexity, *Proc. of the 26th ACM Symp. on Theory of Computing (STOC)*, pp. 534-543, 1994. (This is an extended abstract of No. J45.)

[C26] M. Bellare, O. Goldreich, and S. Goldwasser, Incremental Cryptography and Application to Virus Protection, *Proc. of the 27th ACM Symp. on Theory of Computing (STOC)*, pp. 45-56, 1995.

[C27] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, Private Information Retrieval, *Proc. of the 36th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 41-50, 1995. (This is an extended abstract of No. J46.)

[C28] M. Bellare, O. Goldreich and M. Sudan, Free Bits and Non-Approximability, *Proc. of the 36th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 422-431, 1995. (This is an extended abstract of No. J41.)

[C29] O. Goldreich, R. Rubinfeld and M. Sudan, Learning polynomials with queries: the highly noisy case, *Proc. of the 36th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 294-303, 1995. (This is an extended abstract of No. J57.)

[C30] R. Canetti, U. Feige, O. Goldreich and M. Naor, Adaptively Secure Multi-party Computation, *Proc. of the 28th ACM Symp. on Theory of Computing (STOC)*, pp. 639-648, 1996.

[C31] O. Goldreich, S. Goldwasser and D. Ron, Property Testing and its connection to Learning and Approximation, *Proc. of the 37th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 339–348, 1996. (This is an extended abstract of No. J44.)

[C32] O. Goldreich and D. Ron, Property Testing in Bounded Degree Graphs, *Proc. of the 29th ACM Symp. on Theory of Computing (STOC)*, pp. 406–415, 1997. (This is an extended abstract of No. J59.)

[C33] O. Goldreich and S. Goldwasser, On the Limits of Non-Approximability of Lattice Problems, in *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 1–9, 1998. (This is an extended abstract of No. J54.)

[C34] O. Goldreich and D. Ron, A Sublinear Bipartitness Tester for Bounded Degree Graphs, in *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 289–298, 1998. (This is an extended abstract of No. J49.)

[C35] R. Canetti, O. Goldreich and S. Halevi, The Random Oracle Methodology, Revisited, in *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 209–218, 1998. (This is an extended abstract of No. J61.)

[C36] O. Goldreich, A. Sahai and S. Vadhan, Honest-Verifier Statistical Zero-Knowledge Equals General Statistical Zero-Knowledge, in *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 399–408, 1998.

[C37] O. Goldreich, S. Goldwasser, E. Lehman and D. Ron, Testing Monotinicity, in *39th FOCS*, pages 426–435, 1998. (This extended abstract has been merged with an improvement obtained in joint work with Alex Samorodnitsky to yield No. J56.)

[C38] O. Goldreich, D. Ron and M. Sudan, Chinese Remaindering with Errors, in *31st STOC*, pages 225–234, 1999. (This is an extended abstract of No. J55.)

[C39] R. Canetti, O. Goldreich, S. Goldwasser, and S. Micali. Resettable Zero-Knowledge, *Proc. of the 32nd ACM Symp. on Theory of Computing (STOC)*, pages 235–244, 2000.

[C40] O. Goldreich, S. Vadhan and A. Wigderson, On interactive proofs with a laconic provers, in *Proc. of the 28th ICALP*, Springer's LNCS 2076, pages 334–345, 2001. (This is an extended abstract of No. J64.)

[C41] B. Barak, O. Goldreich, S. Goldwasser and Y. Lindell, Resettably-Sound Zero-Knowledge and its Applications, in *Proc. of the 42th FOCS*, pages 116–125, 2001.

[C42] O. Goldreich and L. Trevisan, Three Theorems regarding Testing Graph Properties, in *Proc. of the 42th FOCS*, pages 460–469, 2001. (This is an extended abstract of No. J63.)

[C43] O. Goldreich, Concurrent Zero-Knowledge With Timing, Revisited, in *Proc. of the 34th STOC*, pages 332–340, 2002.

[C44] O. Goldreich and M. Sudan, Locally Testable Codes and PCPs of Almost-Linear Length, in *Proc. of the 43rd FOCS*, pages xxx–xxx, 2002.

Special Area Conferences (e.g. CRYPTO, PODC, CCC)

[C44] S. Even, O. Goldreich, and A. Lempel, A Randomized Protocol for Signing Contracts, in *Advances in Cryptology: Proceedings of Crypto82*, (D. Chaum et al. editors), Plenum Press, pp. 205–210, 1983. (This is an extended abstract of No. J4.)

[C45] S. Even and O. Goldreich, On The Security of Multi-Party Ping-Pong Protocols, in *Advances in Cryptology: Proceedings of Crypto82*, (D. Chaum et al. editors), Plenum Press, p. 315, 1983. (This is an abstract of No. C1.)

[C46] S. Even and O. Goldreich, On the Power of Cascade Ciphers, in *Advances in Cryptology: Proceedings of Crypto83*, (D. Chaum editor), Plenum Press, pp. 43–50, 1984. (This is an extended abstract of No. J5.)

[C47] O. Goldreich, A Simple Protocol for Signing Contracts, in *Advances in Cryptology: Proceedings of Crypto83*, (D. Chaum editor), Plenum Press, pp. 133–136, 1984.

[C48] S. Even, O. Goldreich, and Y. Yacobi, Electronic Wallet, in *Advances in Cryptology: Proceedings of Crypto83*, (D. Chaum editor), Plenum Press, pp. 383–386, 1984.

[C49] S. Even, O. Goldreich, and Y. Yacobi, Electronic Wallet, in *1984 International Zurich Seminar on Digital Communication*, IEEE Cat. No. 84CH1998-4, pp. 199–201, March 1984. (This is an extended abstract of No. J48.)

[C50] O. Goldreich, On Concurrent Identification Protocols, in *Advances in Cryptology: Proceedings of Eurocrypt84*, (T. Beth et. al. eds.), Lecture Note in Computer Science (209) Springer Verlag, pp. 387–396, 1985.

[C51] O. Goldreich, On the Number of Close-and-Equal Bits in a String (with Implications on the Security of RSA's L.S.B), in *Advances in Cryptology: Proceedings of Eurocrypt84*, (T. Beth et. al. eds.), Lecture Note in Computer Science (209) Springer Verlag, pp. 127–141, 1985.

[C52] O. Goldreich, S. Goldwasser and S. Micali, On the Cryptographic Applications of Random Functions, in *Advances in Cryptology – Crypto '84 (Proceedings)*, (G.R. Blakely et. al. eds.), Lecture Note in Computer Science (196) Springer Verlag, pp. 276–288, 1985.

[C53] B. Chor, and O. Goldreich, RSA/Rabin Least Significant Bits are $1/2 + 1/poly(logN)$-Secure, in *Advances in Cryptology – Crypto '84 (Proceedings)*, (G.R. Blakely et. al. eds.), Lecture Note in Computer Science (196) Springer Verlag, pp. 303–313, 1985.

[C54] S. Even, O. Goldreich and A. Shamir, On the Security of Ping-Pong Protocols when Implemented Using the RSA, in *Advances in Cryptology – Crypto '85 (Proceedings)*, (H.C. Williams ed.), Lecture Note in Computer Science (218) Springer Verlag, pp. 58–72, 1986.

[C55] B. Chor, O. Goldreich and S. Goldwasser, The Bit Security of Modular Squaring given Partial Factorization of the Modulus, in *Advances in Cryptology – Crypto '85 (Proceedings)*, (H.C. Williams ed.), Lecture Note in Computer Science (218) Springer Verlag, pp. 448–457, 1986.

[C56] O. Goldreich and L. Shrira, The Effect of Link Failures on Computation in Asynchronous Rings, *5th ACM Symp. on Principles of Distributed Computing (PODC)*, pp. 174–185, 1986. (This is an extended abstract of No. J7 and J20.)

[C57] O. Goldreich, Two Remarks Concerning the GMR Signature Scheme, in *Advances in Cryptology – Crypto '86 (Proceedings)*, (A.M. Odlyzko ed.), Lecture Note in Computer Science (263) Springer Verlag, pp. 104–110, 1987.

[C58] O. Goldreich, S. Micali, and A. Wigderson, How to Prove All NP Statements in Zero-Knowledge and a Methodology of Cryptographic Protocol Design, in *Advances in Cryptology – Crypto '86 (Proceedings)*, (A.M. Odlyzko ed.), Lecture Note in Computer Science (263) Springer Verlag, pp. 171–185, 1987. (This is an extended abstract of No. J18.)

[C59] O. Goldreich, Towards a Theory of Software Protection, in *Advances in Cryptology – Crypto '86 (Proceedings)*, (A.M. Odlyzko ed.), Lecture Note in Computer Science (263) Springer Verlag, pp. 426–439, 1987. (This is a preliminary version of No. C8.)

[C60] R. Bar-Yehuda, O. Goldreich, A. Itai, On the Time-Complexity of Broadcast in Radio Networks: An Exponential Gap Between Determinism and Randomization, *6th ACM Symp. on Principles of Distributed Computing (PODC)*, 1987, pp. 98–108. (This is an extended abstract of No. J24.)

[C61] O. Goldreich and S. Micali, Zero Knowledge and the Design of Secure Protocols, appeared in the proceedings of *Globecom87*, 1987.

[C62] O. Goldreich and R. Vainish, How to Solve any Protocol Problem – An Efficiency Improvement, in *Advances in Cryptology – Crypto '87 (Proceedings)*, (C. Pomerance ed.), Lecture Note in Computer Science (293) Springer Verlag, pp. 73–86, 1988.

[C63] B. Awerbuch, O. Goldreich, D. Peleg, and R. Vainish, Trade-off Between Information and Communication in Broadcast Protocols, appeared in the proceedings of the *Aegian Workshop on Complexity (AWOC)*, third international workshop on parallel computation and VLSI theory, Korfu, Greece, (1988). (This is an extended abstract of No. J15.)

[C64] Ben-Or, M., O. Goldreich, S. Goldwasser, J. Hastad, J. Kilian, S. Micali, and P. Rogaway, Everything Provable is Provable in Zero-Knowledge, in *Advances in Cryptology – Crypto '88 (Proceedings)*, Lecture Note in Computer Science (403) Springer Verlag, pp. 37–56, 1990.

[C65] Goldreich, O., and E. Kushilevitz, A Perfect Zero-Knowledge Proof for a Decision Problem Equivalent to Discrete Logarithm, in *Advances in Cryptology – Crypto '88 (Proceedings)*, Lecture Note in Computer Science (403) Springer Verlag, pp. 57–70, 1990. (This is an extended abstract of No. J26.)

[C66] O. Goldreich, H. Krawczyk, and M. Luby, On the Existence of Pseudorandom Generators, in *Advances in Cryptology – Crypto '88 (Proceedings)*, Lecture Note in Computer Science (403) Springer Verlag, pp. 146–162, 1990. (This is an extended abstract of No. J28.)

[C67] S. Ben-David, B. Chor, O. Goldreich, and M. Luby, On the Theory of Average Case Complexity, *Proc. of the 4th conf. on Structure in Complexity Theory*, (This is an abstract of No. C13.)

[C68] R. Bar-Yehuda, O. Goldreich, and A. Itai. Efficient Emulation of Single-Hop Radio Network with Collision Detection on Multi-Hop Radio Network with no Collision Detection, *3rd International Workshop*, Nice, France, (proceedings), Lecture Notes in Computer Science, Vol. 392, Springer Verlag, 1989, pp. 24–32. (This is an extended abstract of No. J19.)

[C69] O. Goldreich, A. Herzberg, and Y. Mansour, Source to Destination Communication in the Presence of Faults, *8th ACM Symp. on Principles of Distributed Computing (PODC)*, 1989, pp. 85–102.

[C70] O. Goldreich, and H. Krawczyk, On Sparse Pseudorandom Ensembles, *Advances in Cryptology – Crypto '89 (Proceedings)*, Lecture Note in Computer Science (435) Springer Verlag, pp. 113–127, 1990. (This is an extended abstract of No. J22.)

[C71] S. Even, O. Goldreich, and S. Micali, On-line/Off-line Digital signatures, *Advances in Cryptology – Crypto '89 (Proceedings)*, Lecture Note in Computer Science (435) Springer Verlag, pp. 263–277, 1990. (This is an extended abstract of No. J34.)

[C72] B. Awerbuch, O. Goldreich, and A. Herzberg, A Quantitative Approach to Dynamic Networks, *9th ACM Symp. on Principles of Distributed Computing (PODC)*, pp. 189–204, 1990.

[C73] O. Goldreich and D. Sneh, On the Complexity of Global Computation in the Presence of Link Failures: the case of Unidirectional Faults, *11th ACM Symp. on Principles of Distributed Computing (PODC)*, pp. 103–111, 1992.

[C74] M. Bellare and O. Goldreich, On Defining Proofs of Knowledge, *Advances in Cryptology – Crypto '92 (Proceedings)*, Lecture Note in Computer Science (740) Springer Verlag, pp. 390–420, 1993.

[C75] M. Bellare, O. Goldreich, and S. Goldwasser, Incremental Cryptography: the Case of Hashing and Signing, *Advances in Cryptology – Crypto '94 (Proceedings)*, Lecture Note in Computer Science (839) Springer Verlag, pp. 216–233, 1994.

[C76] I. Damgard, O. Goldreich, T. Okamoto and A. Wigderson, Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs, *Advances in Cryptology – Crypto '95 (Proceedings)*, Lecture Note in Computer Science (963) Springer Verlag, pp. 325–338, 1995.

[C77] S. Decatur, O. Goldreich, and D. Ron, Computational Sample Complexity, *10th COLT*, pp. 130-142, 1997. (This is a preliminary version of No. J52.)

[C78] O. Goldreich and S. Safra, A Combinatorial Consistency Lemma with application to the PCP Theorem, proceedings of *Random97*, Springer LNCS, Vol. 1269, pp. 67–84. (This is a preliminary version of No. J53.)

[C79] O. Goldreich, S. Goldwasser and S. Halevi, Public-Key Cryptosystems from Lattice Reduction Problems, proceedings of *Crypto97*, Springer LNCS, Vol. 1294, pp. 112–131.

[C80] O. Goldreich, S. Goldwasser and S. Halevi, Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem, proceedings of *Crypto97*, Springer LNCS, Vol. 1294, pp. 105–111.

[C81] O. Goldreich and M. Sudan, Computational Indistinguishability: A Sample Hierarchy, proceedings of *13th IEEE Conference on Computational Complexity*, pages 24-33, 1998. (This is an extended abstract of No. J51.)

[C82] O. Goldreich, B. Pfitzmann and R. L. Rivest, Self-Delegation with Controlled Propagation – or – What If You Lose Your Laptop, proceedings of *Crypto98*, Springer LNCS, Vol. 1462, pages 153–168.

[C83] O. Goldreich and S. Vadhan, Comparing Entropies in Statistical Zero-Knowledge with Applications to the Structure of SZK, proceedings of *14th IEEE Conference on Computational Complexity*, pages 54–73, 1999.

[C84] Z. Bar-Yossef, O. Goldreich, and A. Wigderson, Deterministic Amplification of Space Bounded Probabilistic Algorithms, proceedings of *14th IEEE Conference on Computational Complexity*, pages 188–198, 1999.

[C85] O. Goldreich, A. Sahai and S. Vadhan, Can Statistical Zero-Knowledge be Made Non-Interactive? or On the Relationship of SZK and NISZK, Proceedings of *Crypto99*, Springer LNCS, Vol. 1666, pages 467–484.

[C86] M. Bellare, O. Goldreich and H. Krawczyk, Beyond the Birthday Barrier, Without Counters, Proceedings of *Crypto99*, Springer LNCS, Vol. 1666, pages 270–287.

[C87] O. Goldreich and A. Wigderson, Improved Derandomization of BPP using a Hitting Set Generator, Proceedings of *Random99*, Springer LNCS, Vol. 1671, pages 131–137.

[C88] Y. Dodis, O. Goldreich, E. Lehman, S. Raskhodnikova, D. Ron and A. Samorodnitsky, Improved Testing Algorithms for Monotonicity, Proceedings of *Random99*, Springer LNCS, Vol. 1671, pages 97–108.

[C89] O. Goldreich and A. Wigderson, On Pseudorandomness with respect to Deterministic Observers, *Random00, proceedings of the satellite workshops of the 27th ICALP*, Carleton Scientific (Proc. in Inform. 8), pages 77–84, 2000.

[C90] O. Goldreich and Y. Lindell, Session-Key Generation using Human Passwords Only, Proceedings of *Crypto01*, pages 408–432. (This is an extended abstract of No. J62.)

[C91] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, On the (Im)possibility of Software Obfuscation, Proceedings of *Crypto01*, pages 1–18.

[C92] O. Goldreich, H. Karloff, L. Schulman and L. Trevisan, Lower Bounds for Linear Locally Decodable Codes and Private Information Retrieval, in the proceedings of *17th IEEE Conference on Computational Complexity*, pages 175–183, 2002.

[C93] B. Barak and O. Goldreich, Universal arguments and their applications, in the proceedings of *17th IEEE Conference on Computational Complexity*, pages 194–203, 2002.

[C94] O. Goldreich and A. Wigderson, Derandomization that is rarely wrong from short advice that is typically good, in the proceedings of *RANDOM*, pages xxx–xxx, 2002.

4 Survey Papers

Chapters in Books

[S1] Randomness, Interaction, Proofs and Zero-Knowledge, in *The Universal Turing Machine: A Half-Century Survey*, R. Herken (ed.), Oxford University Press, London, 1988. Pages 377–406.

[S2] A Taxonomy of Proof Systems, in *Complexity Theory Retrospective II*, L.A. Hemaspaandra and A. Selman (eds.), Springer, 1997. Pages 109–134.

[S3] Combinatorial Property Testing – A Survey, in *DIMACS Series in Disc. Math. and Theoretical Computer Science*, Vol. 43 (Randomization Methods in Algorithm Design), 1998. Pages 45–59.

[S4] Fundamentals of Cryptography (Chap. 97.2), in *The Electrical Engineering Handbook*, CRC Press, 2000.

[S5] Property Testing in Massive Graphs, in *Handbook of Massive Data Sets*, Kluwer, 2002. Pages 123–147.

[S6] Computational Complexity, in *Mathematics Unlimited – 2001 and Beyond*, Springer, 2001. Pages 507–524.

[S7] Pseudorandomness – Part I, in *IAS/Park City Mathematics Series*, Vol. 10, 2000.

Published in Periodicals or Conference Proceedings

[S8] A Taxonomy of Proof Systems, guest column, in two parts. Part 1 in *Sigact News – Complexity Theory Column 3*, Vol. 24, No. 4, December 1993, pp. 2–13. Part 2 in *Sigact News – Complexity Theory Column 4*, Vol. 25, No. 1, March 1994, pp. 22–30. (This is a preliminary version of No. S2.)

[S9] What is an Envelope, *Almost 2000* (a popular journal for Science and Technology), Vol. 1, pp. 15–17, 1994, (in Hebrew).

[S10] Probabilistic Proof Systems, in the *Proceedings of the International Congress of Mathematicians 1994*, Birkhäuser Verlag, Basel, 1995, pp. 1395–1406.

[S11] On the Foundations of Modern Cryptography (essay), in the proceedings of *Crypto97*, Springer LNCS, Vol. 1294, pp. 46–74.

(A brief summary has appeared in *CryptoBytes*, the technical newletter of RSA Laboratories, Vol. 3, No. 2, 1997.)

[S12] Pseudorandomness, in *Notices of AMS*, pages 1209–1216, November 1999. (This is an abbreviated version of No. S13.)

[S13] Pseudorandomness, in the *Proc. of the 27th ICALP*, Springer LNCS, Vol. 1853, pages 687–704, 2000.

Electronic posting

[S14] On Yao's XOR-Lemma, *ECCC*, TR95-050, 1995. (With N. Nisan and A. Wigderson.)

[S15] Three XOR-Lemmas – An Exposition, *ECCC*, TR95-056, 1995.

[S16] A Sample of Samplers – A Computational Perspective on Sampling, *ECCC*, TR97-020, May 1997.

[S17] Notes on Levin's Theory of Average-Case Complexity, *ECCC*, TR97-058, 1997.

[S18] On Security Preserving Reductions – Revised Terminology, *Cryptology ePrint Archive*, Report 2000/001, 2000.

ECCC resides at `http://www.eccc.uni-trier.de/eccc/`.

5 Books, Lecture Notes and Related Material

Books

[B1] *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, 1998.
Springer, Volume 17 of the Algorithms and Combinatorics series.

[B2] *Foundations of Cryptography – Basic Tools*, 2001.
Cambridge University Press.

[B3] *Foundations of Cryptography – Basic Applications*, 2002.
In preparation. Working drafts available from
`http://www.wisdom.weizmann.ac.il/~oded/foc-vol2.html`

Lecture Notes

[B4] *Foundations of Cryptography – Class Notes*, 1989.
Computer Science Department, Technion, 184 pages.
(Superseeded by B2 and B3.)

[B5] *Theory of Computation* (draft for textbook in Hebrew), 1989.
Computer Science Department, Technion, 184 pages. (Third edition: 1992.)

[B6] *Introduction to Complexity Theory – Lecture Notes*, 1999.
Department of Computer Science, Weizmann Institute of Science, 353 pages.

[B7] *Randomized Methods in Computation – Lecture Notes*, 2001.
Department of Computer Science, Weizmann Institute of Science, 155 pages.

Other Material

[B8] *Foundations of Cryptography – Fragments of a Book*, 1995.
Department of Computer Science, Weizmann Institute of Science, 292 pages.
(This is a preliminary version of B2.)

6 Other Work

Papers in Electronic Forum (unrefereed)

[O1] M. Bellare and O. Goldreich, Proofs of Computational Ability, August 1992. See also *Theory of Cryptography Library*, `http://philby.ucsd.edu/old.html`, Record Arc-03.

[O2] O. Goldreich, L.A. Levin, and N. Nisan, On Constructing 1-1 One-way Functions, *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, TR95-029, 1995.

[O3] O. Goldreich and A. Wigderson, On the Circuit Complexity of Perfect Hashing, *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, TR96-041, 1996.

[O4] O. Goldreich, S. Goldwasser, and S. Halevi, Collision-Free Hashing from Lattice Problems, *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, TR95-042, 1996.

[O5] O. Goldreich, The Graph Clustering Problem has a Perfect Zero-Knowledge Proof, *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, TR96-054, November 1996. (See J47.)

[O6] O. Goldreich and D. Zuckerman, Another proof that BPP subseteq PH (and more), *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, TR97-045, 1997.

[O7] O. Goldreich, S. Goldwasser, and S. Micali, Interleaved Zero-Knowledge in the Public-Key Model, *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, TR99-024, 1999.

[O8] O. Goldreich, S. Vadhan and A. Wigderson, Simplified Derandomization of BPP using a Hitting Set Generator, *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, TR00-004, 2000.

[O9] O. Goldreich and D. Ron, On Testing Expansion in Bounded-Degree Graphs, *ECCC*, `http://www.eccc.uni-trier.de/eccc/`, TR00-020, 2000.

[O10] O. Goldreich, Candidate One-Way Functions Based on Expander Graphs, *Cryptology ePrint Archive*, Report 2000/063, 2000.

[O11] O. Goldreich, H. Karloff, L. Schulman and L. Trevisan, Lower Bounds for Linear Locally Decodable Codes and Private Information Retrieval, *ECCC*, TR01-080, 2001.

[O12] O. Goldreich, Concurrent Zero-Knowledge With Timing, Revisited, *ECCC*, TR01-091, 2001.

[O13] B. Barak and O. Goldreich, Universal arguments and their applications, *ECCC*, TR01-093, 2001.

[O14] O. Goldreich, Using the FGLSS-reduction to Prove Inapproximability Results for Minimum Vertex Cover in Hypergraphs, *ECCC*, TR01-102, 2001.

[O15] O. Goldreich, Y. Lustig and M. Naor, On Chosen Ciphertext Security of Multiple Encryptions,

Research Reports (which did not appear elsewhere)

[O16] O. Goldreich, Graph Partition into Equinumerous Connected Components is NP-Complete, TR No. 202, Computer Science Department, Technion, Haifa, Israel, 1981.

[O17] O. Goldreich, A Protocol for Sending Certified Mail, TR No. 239, Computer Science Department, Technion, Haifa, Israel, 1982.

[O18] O. Goldreich, On the Power of non-binary Block-Ciphers, TR No. 264, Computer Science Department, Technion, Haifa, Israel, 1983.

[O19] O. Goldreich, Sending Certified Mail Using Oblivious Transfer and a Threshold Scheme, TR No. 325, Computer Science Dept, Technion, Haifa, Israel, 1984.

Unpublished Manuscripts (cited by other researchers)

[O20] O. Goldreich, Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle is NP-Hard, July 1984.

[O21] O. Goldreich and S. Micali, The Weakest Pseudo-Random Generator Implies the Strongest One, October 1984.

[O22] O. Goldreich and Y. Moses, Finding a Second Solution is NP-Complete for Almost All Known NPC Problems, May 1986.