List of Publications

Oded Goldreich

January 2, 2024

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, in *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, 2000.

[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.

[J60] O. Goldreich and V. Rosen, On the Security of Modular Exponentiation with Application to the Construction of Pseudorandom Generators, *Jour. of Cryptology*, Vol. 16, pages 71–93, 2003.

[J61] N. Alon, O. Goldreich and Y. Mansour. Almost k-wise independence versus k-wise independence, *IPL*, Vol. 88 (3), pages 107–110, June 2003.

[J62] O. Goldreich, S. Vadhan and A. Wigderson, On interactive proofs with a laconic provers, *Computational Complexity*, Vol. 11, pages 1–53, 2002.

[J63] O. Goldreich and L. Trevisan, Three Theorems regarding Testing Graph Properties, *Random Structures and Algorithms*, Vol. 23 (1), pages 23–57, August 2003.

[J64] R. Canetti, O. Goldreich and S. Halevi, The Random Oracle Methodology, Revisited, *Jour. of the ACM*, Vol. 51 (4), pages 557–594, July 2004.

[J65] O. Goldreich, Concurrent Zero-Knowledge With Timing, Revisited, In *Theoretical Computer Science: Essays in Memory of Shimon Even*, Festschrift series of Springer's LNCS (as Vol 3895), pages 27–87, March 2006.

[J66] O. Goldreich and Y. Lindell, Session-Key Generation using Human Passwords Only, *Jour. of Cryptology*, pages 241–340, Summer 2006.

[J67] O. Goldreich and M. Sudan, Locally Testable Codes and PCPs of Almost-Linear Length, *JACM*, Vol. 53, No. 4, July 2006, pp. 558–655.

[J68] O. Goldreich, H. Karloff, L. Schulman and L. Trevisan, Lower Bounds for Linear Locally Decodable Codes and Private Information Retrieval, *Computational Complexity*, Vol. 15, No. 3, Pages 263–296, October 2006.

[J69] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Robust PCPs of Proximity, Shorter PCPs and Applications to Coding, *SICOMP*, Volume 36, Issue 4, pages 889–974, 2006.

[J70] O. Goldreich and D. Ron, Approximating average parameters of graphs, *Random Structures and Algorithms*, Volume 32, Number 3, pages 473–493, 2008.

[J71] B. Barak and O. Goldreich, Universal arguments and their applications, *SICOMP*, Volume 38, Issue 5, pages 1661–1694, 2008.

[J72] O. Goldreich, On Expected Probabilistic Polynomial-Time Adversaries – A suggestion for restricted definitions and their benefits, *Journal of Cryptology*, Volume 23, Issue 1, pages 1–36, 2010.

[J73] O. Goldreich and O. Sheffet, On the randomness complexity of property testing, *Computational Complexity*, Volume 19, Number 1, pages 99–133, 2010.

[J74] O. Goldreich, S. Goldwasser and A. Nussboim. On the Implementation of Huge Random Objects, *SICOMP*, Vol. 39, No. 7, pages 2761–2822, 2010.

[J75] O. Goldreich and D. Ron, Algorithmic Aspects of Property Testing in the Dense Graphs Model, *SICOMP*, Vol. 40, No. 2, pages 376–445, 2011.

[J76] O. Goldreich and D. Ron, On Proximity Oblivious Testing, *SICOMP*, Vol. 40, No. 2, pages 534–566, 2011.

[J77] D. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev, More Constructions of Lossy and Correlation-Secure Trapdoor Functions, *Journal of Crypto.*, Vol. 26 (1), pages 39–74, 2013. Online First, 10-Nov-2011.

[J78] O. Goldreich and O. Meir, The Tensor Product of Two Good Codes Is Not Necessarily Robustly Testable, *IPL*, Vol. 112, pages 351–355, 2012.

[J79] O. Goldreich, M. Krivelevich, I. Newman, and E. Rozenberg, Hierarchy Theorems for Property Testing, *Computational Complexity*, Vol. 21 (1), pages 129-192, 2012.

[J80] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, On the (Im)possibility of Software Obfuscation, *Journal of ACM*, Vol. 59, No. 2, Art. 6, April 2012.

[J81] O. Goldreich, B. Juba, and M. Sudan, A Theory of Goal-Oriented Communication, *Journal of ACM*, Vol. 59, No. 2, Art. 8, April 2012.

[J82] O. Goldreich and R. Izsak. Monotone Circuits: One-Way Functions versus Pseudorandom Generators, *ToC*, Vol. 8, Art. 10, pages 231–238, 2012.

[J83] A. Czumaj, O. Goldreich, D. Ron, C. Seshadhri, A. Shapira, and C. Sohler, Finding Cycles and Trees in Sublinear Time, *RS&A*, Vol. 45, Nr. 2, pages 139–184, 2014. Article first published online: 22-Aug-2012.

[J84] O. Goldreich and R. Rothblum, Enhancements of Trapdoor Permutations, *Journal of Cryptology*, Vol. 6, Nr. 3, pages 484–512, 2013. Online First, 12-Sept-2012.

[J85] O. Goldreich and I. Shinkar. Two-Sided Error Proximity Oblivious Testing, *Random Structures and Algorithms*, Vol. 48 (2), pages 341–383, 2016.

[J86] O. Goldreich and O. Meir. Input-Oblivious Proof Systems and a Uniform Complexity Perspective on P/poly, *TOCT*, Vol. 7(4), Art. 16, 2015.

[J87] O. Goldreich and D. Ron. On Sample-Based Testers, *TOCT*, Vol. 8(2), 2016.

[J88] O. Goldreich and A. Tal. Matrix Rigidity of Random Toeplitz Matrices, *Computational Complexity*, 27 (2), pages 305–350, 2018.

[J89] O. Goldreich and D. Ron. On Learning and Testing Dynamic Environments, *JACM*, Vol. 64 (3), pages 21:1–21:90, 2017.

[J90] O. Goldreich, T. Gur, and R. Rothblum. Proofs of Proximity for Context-Free Languages and Read-Once Branching Programs, *Inform. and Comput.*, Vol. 261 (Part 2), pages 175–201, 2018.

[J91] O. Goldreich and T. Gur. Universal Locally Testable Codes, *CJTCS*, Vol. 2018, Art. 3.

[J92] O. Goldreich, T. Gur, and I. Komargodski. Strong Locally Testable Codes with Relaxed Local Decoders, *ACM Transactions on Computation Theory*, Vol. 11 (3), pages 17:1–17:38, 2019.

[J93] O. Goldreich. Hierarchy Theorems for Testing Properties in Size-Oblivious Query Complexity, *Computational Complexity*, Vol. 28 (4), pages 709–747, 2019.

[J94] O. Goldreich and D. Ron. The Subgraph Testing Model, *ACM Transactions on Computation Theory*, Vol. 12, No. 4, Article 28. October 2020.

[J95] O. Goldreich and T. Gur. Universal Locally Verifiable Codes and 3-Round Interactive Proofs of Proximity for CSP, *Theoretical Computer Science*, Vol. 878–879, pages 83–101, 2021.

[J96] O. Goldreich. Improved bounds on the AN-complexity of O(1)-linear functions, *Computational Complexity*, Vol. 31 (2), Art. 7, 2022.

[J97] O. Goldreich and A. Wigderson. Robustly Self-Ordered Graphs: Constructions and Applications to Property Testing, *TheoretiCS*, Vol. 1, Art. 1, 2022.

[J98] O. Goldreich and D. Ron. A Lower Bound on the Complexity of Testing Grained Distributions, *Computational Complexity*, Vol. 32 (2), Art. 11, 2023.

[J99] O. Goldreich and D. Ron. Testing Distributions of Huge Objects, *TheoretiCS*, Vol. 2, Art. 12, 2023.

In Press

[J100] O. Goldreich and A. Wigderson. Good Permutation Codes Based on the Shuffle-Exchange Network, Israel Journal of Mathematics

3 Original Papers in (Refereed) Conference Proceedings

The paper are ordered by the date of the conferences, and not by the date of the publication of its proceedings. This comment is relevant with respect to the early Crypto' conferences (i.e., of the 1980's). Also, till the late 1980's, simultanous publication in various conferences was allowed (and even encouraged).

[C1] 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.)

[C2] 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. C6.)

[C3] 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.)

[C4] O. Goldreich, A Simple Protocol for Signing Contracts, in *Advances in Cryptology: Proceedings of Crypto83*, (D. Chaum editor), Plenum Press, pp. 133–136, 1984.

[C5] 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.

[C6] 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.

[C7] 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 version is related to No. C5.)

[C8] 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.

[C9] 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. (This is an extended abstract of No. J14.)

[C10] 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.

[C11] 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.

[C12] 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.)

[C13] 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.)

[C14] 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.

[C15] 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.

[C16] 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.)

[C17] 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.

[C18] 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.)

[C19] 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.)

[C20] 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.

[C21] 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.)

[C22] 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. C24.)

[C23] 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.)

[C24] 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.)

[C25] 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.

[C26] 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.)

[C27] O. Goldreich and S. Micali, Zero Knowledge and the Design of Secure Protocols, appeared in the proceedings of *Globecom87*, 1987.

[C28] 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.

[C29] 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.)

[C30] 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.)

[C31] 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.

[C32] 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.)

[C33] 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.)

[C34] 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.

[C35] 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. C37.)

[C36] 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.

[C37] 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.)

[C38] 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.)

[C39] 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.

[C40] 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.)

[C41] 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.)

[C42] 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.

[C43] 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.)

[C44] 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.

[C45] 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.)

[C46] 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.)

[C47] 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.)

[C48] 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.)

[C49] 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.)

[C50] 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.)

[C51] 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.

[C52] 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.

[C53] 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.

[C54] 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.

[C55] 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.)

[C56] 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.)

[C57] 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.

[C58] 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.

[C59] 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.

[C60] 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.)

[C61] 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.)

[C62] 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.)

[C63] 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.

[C64] 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.)

[C65] 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.)

[C66] S. Decatur, O. Goldreich, and D. Ron, Computational Sample Complexity, *10th COLT*, pp. 130-142, 1997. (This is a preliminary version of No. J52.)

[C67] 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.)

[C68] O. Goldreich, S. Goldwasser and S. Halevi, Public-Key Cryptosystems from Lattice Reduction Problems, proceedings of *Crypto97*, Springer LNCS, Vol. 1294, pp. 112–131.

[C69] 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.

[C70] 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.)

[C71] 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.)

[C72] 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. J64.)

[C73] 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.

[C74] 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.)

[C75] 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.

[C76] 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.)

[C77] 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.)

[C78] 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.

[C79] 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.

[C80] 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.

[C81] M. Bellare, O. Goldreich and H. Krawczyk, Beyond the Birthday Barrier, Without Counters, Proceedings of *Crypto99*, Springer LNCS, Vol. 1666, pages 270–287.

[C82] O. Goldreich and A. Wigderson, Improved Derandomization of BPP using a Hitting Set Generator, Proceedings of *Random99*, Springer LNCS, Vol. 1671, pages 131–137.

[C83] 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.

[C84] 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.

[C85] 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.

[C86] 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. J62.)

[C87] 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. J66.)

[C88] 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. (This is an extended abstract of No. J80.)

[C89] 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.

[C90] 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.)

[C91] O. Goldreich, Concurrent Zero-Knowledge With Timing, Revisited, in *Proc. of the 34th STOC*, pages 332–340, 2002. (This is an extended abstract of No. J65.)

[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. (This is an extended abstract of No. J68.)

[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. (This is an extended abstract of No. J71.)

[C94] O. Goldreich and A. Wigderson, Derandomization that is rarely wrong from short advice that is typically good, in the proceedings of *RANDOM*, Springer LNCS, Vol. 2483, pages 209–223, 2002.

[C95] O. Goldreich and M. Sudan, Locally Testable Codes and PCPs of Almost-Linear Length, in *Proc. of the 43rd FOCS*, pages 13–22, 2002. (This is an extended abstract of No. J67.)

[C96] E. Ben-Sasson, O. Goldreich and M. Sudan, Bounds on 2-Query Codeword Testing, in the proceedings of *RANDOM*, Springer LNCS, Vol. 2764, pages 216–227, 2003.

[C97] O. Goldreich, S. Goldwasser and A. Nussboim. On the Implementation of Huge Random Objects, in *Proc. of 44th FOCS*, pages 68–79, 2003. (This is an extended abstract of No. J74.)

[C98] R. Canetti, O. Goldreich and S. Halevi, On the random-oracle methodology as applied to length-restricted signature schemes, in the proceedings of the *1st Theory of Cryptography Conference*, Springer LNCS, Vol. 2951, pages 40–57, 2004.

[C99] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Robust PCPs of Proximity, Shorter PCPs and Applications to Coding, in *Proc. of the 36th STOC*, pages 1-10, 2004. (This is an extended abstract of No. J69.)

[C100] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Short PCPs Verifiable in Polylogarithmic Time, in the proceedings of *20th IEEE Conference on Computational Complexity*, pages 120–134, 2005.

[C101] O. Goldreich and D. Ron, Approximating Average Parameters of Graphs, in the proceedings of *10th RANDOM*, Springer LNCS, Vol. 4110, pages 363–374, 2006. (This is an extended abstract of No. J70.)

[C102] A. Akavia, O. Goldreich, S. Goldwasser and D. Moshkovitz On Basing One-Way Functions on NP-Hardness, Proceedings of the *38th STOC*, pages 701–710, 2006.

[C103] O. Goldreich, On Expected Probabilistic Polynomial-Time Adversaries – A suggestion for restricted definitions and their benefits, in the proceedings of the *4th Theory of Cryptography Conference*, Springer LNCS, Vol. 4392, pages 174–193, 2007. (This is an extended abstract of No. J72.)

[C104] O. Goldreich and O. Sheffet, On the randomness complexity of property testing, in the proceedings of *11th RANDOM*, Springer LNCS, Vol. 4627, pages 296–310, 2007. (This is an extended abstract of No. J73.)

[C105] K. Barhum, O. Goldreich and A. Shraibman, On approximating the average distance between points, in the proceedings of *11th RANDOM*, Springer LNCS, Vol. 4627, pages 509–524, 2007.

[C106] O. Goldreich and D. Ron, On Proximity Oblivious Testing, Proceedings of the *41st STOC*, pages 141–150, 2009. (This is an extended abstract of No. J76.)

[C107] O. Goldreich and D. Ron, Algorithmic Aspects of Property Testing in the Dense Graphs Model, in the proceedings of *13th RANDOM*, Springer LNCS, Vol. 5687, pages 520–533, 2009. (This is an extended abstract of No. J75.)

[C108] O. Goldreich, M. Krivelevich, I. Newman, and E. Rozenberg, Hierarchy Theorems for Property Testing, in the proceedings of *13th RANDOM*, Springer LNCS, Vol. 5687, pages 504-519, 2009. (This is an extended abstract of No. J79.)

[C109] D. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev, More Constructions of Lossy and Correlation-Secure Trapdoor Functions, in the proceedings of *13th PKC*,

Springer LNCS, Vol. 6056, pages 279–295, 2010. (This is an extended abstract of No. J77.)

[C110] O. Goldreich. On Testing Computability by Small Width OBDDs, in the proceedings of *14th RANDOM*, Springer LNCS, Vol. 6302, pages 574–586, 2010.

[C111] O. Goldreich, B. Juba, and M. Sudan, A Theory of Goal-Oriented Communication, in the proceedings of *30th PODC*, pages 299–300, 2011. (This version is related to No. J81.)

[C112] L. Avigad and O. Goldreich, Testing Graph Blow-Up, in the proceedings of *15th RANDOM*, Springer LNCS, Vol. 6845, pages 389– 399, 2011.

[C113] O. Goldreich and T. Kaufman. Proximity Oblivious Testing and the Role of Invariances, in the proceedings of *15th RANDOM*, Springer LNCS, Vol. 6845, pages 579–592, 2011.

[C114] O. Goldreich and I. Shinkar. Two-Sided Error Proximity Oblivious Testing, in the proceedings of *16th RANDOM*, Springer LNCS, Vol. 7408, pages 565–578, 2012. (This is an extended abstract of No. J85.)

[C115] O. Goldreich, S. Goldwasser, and D. Ron. On the possibilities and limitations of pseudodeterministic algorithms, in the proceedings of the *4th Innovations in Theoretical Computer Science*, pages 127–138, 2013.

[C116] O. Goldreich and A. Wigderson. On Derandomizing Algorithms that Err Extremely Rarely, in the proceedings of *46th STOC*, pages 109–118, 2014.

[C117] O. Goldreich. On Multiple Input Problems in Property Testing, in the proceedings of *18th RANDOM*, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik 2014 LIPIcs ISBN 978-3-939897-74-3, pages 704–720, 2014.

[C118] O. Goldreich and D. Ron. On Learning and Testing Dynamic Environments, in the proceedings of *55th FOCS*, pages 336–343, 2014. (This is an extended abstract of No. J89.)

[C119] O. Goldreich and D. Ron. On Sample-Based Testers, in the proceedings of *6th ITCS*, pages 337–345, 2015. (This is an extended abstract of No. J87.)

[C120] O. Goldreich, T. Gur, and I. Komargodski. Strong Locally Testable Codes with Relaxed Local Decoders, Proceedings of *30th Conference on Computational Complexity*, pages 1–41, 2015. (This is an extended abstract of No. J92.)

[C121] O. Goldreich, E. Viola, and A. Wigderson. On Randomness Extraction in AC0, Proceedings of *30th Conference on Computational Complexity*, pages 601–668, 2015.

[C122] O. Goldreich, T. Gur, and R. Rothblum. Proofs of Proximity for Context-Free Languages and Read-Once Branching Programs, In *42nd ICALP* (1), pages 666–677, 2015. (This is an extended abstract of No. J90.)

[C123] O. Goldreich and A. Tal. Matrix Rigidity of Random Toeplitz Matrices, In *48th STOC*, pages 91–104, 2016. (This is an extended abstract of No. J88.)

[C124] O. Goldreich and G. Rothblum. Simple doubly-efficient interactive proof systems for locally-characterizable sets, Proceedings of *9th ITCS*, pages 18:1–18:19, 2018.

[C125] O. Goldreich and G. Rothblum. Counting t-cliques: Worst-case to average-case reductions and Direct interactive proof systems, Proceedings of *59th FOCS*, pages 77–88, 2018.

[C126] O. Goldreich and D. Ron. The Subgraph Testing Model, Proceedings of *10th ITCS*, pages 37:1–37:19, 2019. (This is an extended abstract of No. J94.)

[C127] I. Dinur, O. Goldreich, and T. Gur. Every set in P is strongly testable under a suitable encoding, Proceedings of *10th ITCS*, pages 30:1–30:17, 2019.

[C128] O. Goldreich. Testing Graphs in Vertex-Distribution-Free Models, Proceedings of *51st STOC*, pages 527–534, 2019.

[C129] O. Goldreich and A. Wigderson. Robustly Self-Ordered Graphs: Constructions and Applications to Property Testing, Proceedings of *36th Conference on Computational Complexity*, pages 12:1–12:74, 2021. (This is an extended abstract of No. J97.)

[C130] M. Ball, O. Goldreich, and T. Malkin. Communication Complexity with Defective Randomness, Proceedings of *36th Conference on Computational Complexity*, pages 14:1–14:10, 2021.

[C131] O. Goldreich and A. Wigderson. Non-adaptive vs Adaptive Queries in the Dense Graph Testing Model, Proceedings of *62nd FOCS*, pages 269–275, 2022.

[C132] M. Ball, O. Goldreich, and T. Malkin. Randomness Extraction from Somewhat Dependent Sources, Proceedings of *13th ITCS*, pages 12:1–12:14, 2022.

[C133] O. Goldreich and D. Ron. Testing Distributions of Huge Objects, Proceedings of *13th ITCS*, pages 78:1–78:19, 2022. (This is an extended abstract of No. J99.)

[C134] O. Goldreich, G. Rothblum, and T. Skverer. On Interactive Proofs of Proximity with Proof-Oblivious Queries, Proceedings of *14th ITCS*, pages 59:1–59:16, 2023.

4 Other Work

This section only lists works that are not listed in the prior sections. Likewise, works are listed in the first relevant subsection. In all cases, these publications were not refereed.

4.1 Collected Works (LNCS Vol. 6650, 2011)

The works collected in this volume were compeleted at different times, and were revised towards this publication. The year of the original version is mentioned in square brackets.

[O1] O. Goldreich, Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle is NP-Hard [1984]

[O2] M. Bellare and O. Goldreich, Proofs of Computational Ability [1992]

[O3] O. Goldreich, L.A. Levin, and N. Nisan, On Constructing 1-1 One-way Functions [1995]

[O4] O. Goldreich and A. Wigderson, On the Circuit Complexity of Perfect Hashing [1996]

[O5] O. Goldreich, S. Goldwasser, and S. Halevi, Collision-Free Hashing from Lattice Problems [1996]

[O6] O. Goldreich and D. Zuckerman, Another proof that BPP subseteq PH (and more) [1997]

[O7] O. Goldreich, Strong Proofs of Knowledge [1999]

[O8] O. Goldreich, S. Vadhan and A. Wigderson, Simplified Derandomization of BPP using a Hitting Set Generator [2000]

[O9] O. Goldreich and D. Ron, On Testing Expansion in Bounded-Degree Graphs [2000]

[O10] O. Goldreich, Candidate One-Way Functions Based on Expander Graphs [2000]

[O11] O. Goldreich, Using the FGLSS-reduction to Prove Inapproximability Results for Minimum Vertex Cover in Hypergraphs [2001]

[O12] O. Goldreich. The GGM Construction does NOT yield Correlation Intractable Function Ensembles [2002]

[O13] O. Goldreich, M. Sudan and L. Trevisan, From logarithmic advice to single-bit advice [2004]

[O14] M. Bellare and O. Goldreich, On Probabilistic versus Deterministic Provers in the Definition of Proofs Of Knowledge [2006]

[O15] O. Goldreich, On the Average-Case Complexity of Property Testing [2007]

[O16] O. Goldreich, A Candidate Counterexample to the Easy Cylinders Conjecture [2009]

[O17] Z. Brakerski and O. Goldreich, From absolute distinguishability to positive distinguishability [2009]

[O18] O. Goldreich. In a World of P=BPP [2010]

4.2 Collected Works (LNCS Vol. 12050, 2020)

The works collected in this volume were compeleted at different times, and were revised towards this publication. The year of the original version is mentioned in square brackets.

[O19] S. Decatur, O. Goldreich, and D. Ron, A Probabilistic Error-Correcting Scheme that Provides Partial Secrecy [1997]

[O20] O. Goldreich and O. Meir, Bridging a Small Gap in the Gap Amplification of Assignment Testers [2007]

[O21] O. Goldreich, On (Valiant's) Polynomial-Size Monotone Formula for Majority [2011]

[O22] O. Goldreich, Two Comments on Targeted Canonical Derandomizers [2011]

[O23] O. Goldreich, On the Effect of the Proximity Parameter on Property Testers [2012]

[O24] O. Goldreich and A. Wigderson, On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions [2013]

[O25] O. Goldreich, On the Communication Complexity Methodology for Proving Lower Bounds on the Query Complexity of Property Testing [2013]

[O26] O. Goldreich and L. Teichner, Super-Perfect Zero-Knowledge Proofs [2014]

[O27] O. Goldreich and D. Ron, On the Relation between the Relative Earth Mover Distance and the Variation Distance (an exposition) [2016]

[O28] O. Goldreich, The Uniform Distribution is Complete with respect to Testing Identity to a Fixed Distribution [2016]

[O29] O. Goldreich and M. Leshkowitz, On Emulating Interactive Proofs with Public Coins [2016]

[O30] O. Goldreich, Reducing Testing Affine Spaces to Testing Linearity of Functions [2016]

[O31] O. Goldreich, Deconstructing 1-Local Expanders [2016]

[O32] O. Goldreich and G. Rothblum, Worst-Case to Average-Case Reductions for Subclasses of P [2017]

[O33] O. Goldreich, On the Optimal Analysis of the Collision Probability Tester (an exposition) [2017]

[O34] O. Goldreich and A. Tal, On Constant-Depth Canonical Boolean Circuits for Computing Multilinear Functions [2017]

[O35] O. Goldreich and G. Rothblum, Constant-Round Interactive Proof Systems for AC0[2] and NC1 [2018]

[O36] O. Goldreich, Flexible Models for Testing Graph Properties [2018]

[O37] I. Benjamini and O. Goldreich, Pseudo-Mixing Time of Random Walks [2019]

[O38] O. Goldreich, On Constructing Expanders for any Number of Vertices [2019]

4.3 Papers in Electronic Forum

ECCC resides at `https://eccc.weizmann.ac.il`.

[O39] O. Goldreich, The Graph Clustering Problem has a Perfect Zero-Knowledge Proof, *ECCC*, TR96-054, November 1996. (See follow-up J47.)

[O40] O. Goldreich, S. Goldwasser, and S. Micali, Interleaved Zero-Knowledge in the Public-Key Model, *ECCC*, TR99-024, 1999.

[O41] O. Goldreich, Y. Lustig and M. Naor, On Chosen Ciphertext Security of Multiple Encryptions, *Cryptology ePrint Archive*, Report 2002/089, 2002.

[O42] O. Goldreich and D. Ron, "On Estimating the Average Degree of a Graph", *ECCC*, TR04-013, 2004. (See follow-up J70.)

[O43] M. Bellare, O. Goldreich and A. Mityagin, The Power of Verification Queries in Message Authentication and Authenticated Encryption, Cryptology ePrint Archive, Report 2004/309.

[O44] O. Goldreich. Multi-pseudodeterministic algorithms, ECCC TR19-012, 2019.

[O45] O. Goldreich. Testing Bipartitness in an Augmented VDF Bounded-Degree Graph Model, arXiv 1905.03070, 2019.

[O46] O. Goldreich. On the Complexity of Estimating the Effective Support Size, ECCC TR19-088, 2019.

[O47] O. Goldreich. Testing Isomorphism in the Bounded-Degree Graph Model, ECCC TR19-102, 2019.

[O48] O. Goldreich and D. Ron. One-Sided Error Testing of Monomials and Affine Subspaces, ECCC TR20-068, 2020.

[O49] O. Goldreich. On Counting t-Cliques Mod 2, ECCC TR20-104, 2020.

[O50] O. Goldreich. On Testing Hamiltonicity in the Bounded Degree Graph Model, ECCC TR20-109, 2020.

[O51] O. Goldreich. On Testing Asymmetry in the Bounded Degree Graph Model, ECCC TR20-118, 2020.

[O52] O. Goldreich. Robust Self-Ordering versus Local Self-Ordering, ECCC TR21-034, 2021.

[O53] N. Bshouty and O. Goldreich. On properties that are non-trivial to test, ECCC TR22-013, 2022.

[O54] O. Goldreich and L. Tauber. Testing in the bounded-degree graph model with degree bound two, ECCC TR22-184, 2022.

[O55] O. Goldreich. On the Lower Bound on the Length of Relaxed Locally Decodable Codes, ECCC TR23-064, 2023.

[O56] O. Goldreich. On the complexity of enumerating ordered sets, ECCC TR23-134, 2023.

[O57] O. Goldreich and L. Tauber. On Testing Isomorphism to a Fixed Graph in the Bounded-Degree Graph Model, ECCC TR23-146, 2023.

[O58] O. Goldreich. On coarse and fine approximate counting of t-cliques, ECCC TR23-158, 2023.

[O59] O. Goldreich and L. Tauber. On Testing Group Properties, ECCC TR23-214, 2023.

4.4 Reports and Unpublished Manuscripts

Prior to the days of internet, these things were used.

Research Reports

[O60] O. Goldreich, Graph Partition into Equinumerous Connected Components is NP-Complete, TR No. 202, Computer Science Department, Technion, Haifa, Israel, 1981.

[O61] O. Goldreich, A Protocol for Sending Certified Mail, TR No. 239, Computer Science Department, Technion, Haifa, Israel, 1982.

[O62] O. Goldreich, On the Power of non-binary Block-Ciphers, TR No. 264, Computer Science Department, Technion, Haifa, Israel, 1983.

[O63] 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)

[O64] O. Goldreich and S. Micali, The Weakest Pseudo-Random Generator Implies the Strongest One, October 1984.

[O65] O. Goldreich and Y. Moses, Finding a Second Solution is NP-Complete for Almost All Known NPC Problems, May 1986.

5 Survey Papers

5.1 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. Pages 253–285.

[S8] On Promise Problems – A Survey, in *Theoretical Computer Science: Essays in Memory of Shimon Even*, Festschrift series of Springer's LNCS (as Vol 3895), pages 254–290, March 2006.

[S9] Randomness and Computation, in *Handbook of Probability Theory with Applications*, Sage Publishers, 2008. Pages 131–147.

[S10] Computational Complexity (with A. Wigderson), in *The Princeton Companion to Mathematics*, Princeton University Press, pages 575–604, 2008.

[S11] Short Locally Testable Codes and Proofs (Survey), in *Property Testing*, Springer's LNCS, Vol 6390, pages 65–104, 2010.

[S12] Introduction to Testing Graph Properties, in *Property Testing*, Springer's LNCS, Vol 6390, pages 105–141, 2010.

[S13] General Cryptographic Protocols: The Very Basics, in *Secure Multi-Party Computation* (M.M. Prabhakaran and A. Sahai, eds), pages 1–27, IOS Press, Amsterdam, 2013.

[S14] A Short Tutorial of Zero-Knowledge, in *Secure Multi-Party Computation* (M.M. Prabhakaran and A. Sahai, eds), pages 28–60, IOS Press, Amsterdam, 2013.

[S15] On the foundations of cryptography, in *Providing Sound Foundations for Cryptography*, pages 411–496, 2019.

[S16] On the impact of cryptography on complexity theory, in *Providing Sound Foundations for Cryptography*, pages 497–526, 2019.

[S17] On some noncryptographic works of Goldwasser and Micali, in *Providing Sound Foundations for Cryptography*, pages 527–542, 2019.

5.2 Published in Periodicals or Conference Proceedings

[S18] 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.)

[S19] What is an Envelope, *Almost 2000* (a popular journal for Science and Technology), Vol. 1, pp. 15–17, 1994, (in Hebrew).

[S20] Probabilistic Proof Systems, in the *Proceedings of the International Congress of Mathematicians 1994*, Birkhäuser Verlag, Basel, 1995, pp. 1395–1406.

[S21] 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.)

[S22] Pseudorandomness, in *Notices of AMS*, pages 1209–1216, November 1999. (This is an abbreviated version of No. S23.)

[S23] Pseudorandomness, in the *Proc. of the 27th ICALP*, Springer LNCS, Vol. 1853, pages 687–704, 2000.

[S24] Cryptography and Cryptographic Protocols, *PODC Jubilee Issue of Distributed Computing*, Vol. 16, No. 2–3, pages 177–199, 2003.

[S25] Zero-Knowledge: Abstract of a Tutorial, in the *Proc. of the 43rd FOCS*, page 3, 2002. (This is an abstract of No. S26.)

[S26] Zero-Knowledge twenty years after its invention, *Quaderni di Matematica*, Vol. 13 (Complexity of Computations and Proofs, ed. J. Krajicek), pages 249–304, 2004.

[S27] Foundations of Cryptography – A Primer, in *Foundations and Trends in Theoretical Computer Science*, Volume 1, Issue 1, 2005.

[S28] Bravely, Moderately: A Common Theme in Four Recent Results, guest column, in *Sigact News – Complexity Theory Column 51*, Vol. 37, Nr. 2, pages 31-46, June 2006.

[S29] Probabilistic Proof Systems – A Primer, in *Foundations and Trends in Theoretical Computer Science*, Volume 3, Issue 1, 2007.

[S30] Invitation to Complexity Theory, in *XRDS*, Vol. 18, No. 3, Spring 2012.

[S31] On Doubly-Efficient Interactive Proof Systems, in *Foundations and Trends in Theoretical Computer Science*, Volume 13, Issue 3, 2018.

5.3 Collected Works (LNCS Vol. 6650, 2011)

In addition to the surveys listed next, surveys number S9, S11, S12, and S28 also appear in this collection. The surveys collected in this volume were compeleted at different times, and were revised towards this publication. The year of the original version is mentioned in square brackets.

[S32] On Yao's XOR-Lemma (with N. Nisan and A. Wigderson) [1995]

[S33] Three XOR-Lemmas – An Exposition [1995]

[S34] A Sample of Samplers – A Computational Perspective on Sampling [1997]

[S35] Notes on Levin's Theory of Average-Case Complexity [1988 and 1997]

[S36] On Security Preserving Reductions – Revised Terminology [2000]

[S37] On the complexity of computational problems regarding distributions (with S. Vadhan) [2003]

[S38] Basing Non-Interactive Zero-Knowledge on (Enhanced) Trapdoor Permutations: The State of the Art [2008]

[S39] Average Case Complexity, Revisited [2008]

[S40] Basic Facts about Expander Graphs [2008]

[S41] A Brief Introduction to Property Testing [2010]

5.4 Electronic posting

ECCC resides at `https://eccc.weizmann.ac.il`.

[S42] "On the doubly-efficient interactive proof systems of GKR", *ECCC*, TR17-101, June 2017.

[S43] "Overview of the doubly-efficient interactive proof systems of RRR", *ECCC*, TR17-102, June 2017.

[S44] "Open Problems in Property Testing of Graphs", *ECCC*, TR21-088, June 2021.

[S45] "On the Locally Testable Code of Dinur et al. (2021)", *ECCC*, TR21-175, December 2021.

[S46] "The KW Games as a Teaser", *ECCC*, TR21-181, December 2021.

[S47] "On teaching the approximation method for circuit lower bounds", *ECCC*, TR23-034, March 2023.

6 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*, 2004.
Cambridge University Press.

[B4] *Computational Complexity: A Conceptual Perspective*, 2008.
Cambridge University Press.

[B5] *P, NP, and NP-Completeness: The Basics of Complexity Theory*, 2010.
Cambridge University Press.

[B6] *A Primer on Pseudorandom Generators*, 2010.
AMS, ULECT series, Nr. 55.

[B7] *Introduction to Property Testing*, 2017.
Cambridge University Press.

Lecture Notes

[B8] *Foundations of Cryptography – Class Notes*, 1989.
Computer Science Department, Technion, 184 pages.
(Superseeded by B2 and B3.)

[B9] *Theory of Computation* (draft for a textbook in Hebrew), 1989.
Computer Science Department, Technion, 184 pages. (Third edition: 1992.)

[B10] *Introduction to Complexity Theory – Lecture Notes.*

1. For a two-semester course, 353 pages, 1999.
2. For a one-semester course, 104 pages, 2002.

Department of Computer Science and Applied Math., Weizmann Institute of Science.
(Superseeded by B4.)

[B11] *Randomized Methods in Computation – Lecture Notes*, 2001.
Department of Computer Science and Applied Math., Weizmann Institute, 155 pages.

Other Material

[B12] *Foundations of Cryptography – Fragments of a Book*, 1995.
Department of Computer Science and Applied Math., Weizmann Institute, 292 pages.
(This is a preliminary version of B2.)