

Work and Publications

Oded Goldreich

January 24, 2014

- [1] S. Even and O. Goldreich, The Minimum Length Generator Sequence is NP-Hard.
 - *Journal of Algorithms*, vol. 2, pp. 311–313, 1981.
- [2] 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.
- [3] 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.
- [4] S. Even, O. Goldreich, and A. Lempel, A Randomized Protocol for Signing Contracts.
 - *Advances in Cryptology: Proceedings of Crypto82*, (D. Chaum et al. editors), Plenum Press, pp. 205–210, 1983.
 - *Comm. of the ACM*, Vol. 28, No. 6, pp. 637–647, 1985.
- [5] 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.
- [6] O. Goldreich, A Simple Protocol for Signing Contracts.
 - *Advances in Cryptology: Proceedings of Crypto83*, (D. Chaum editor), Plenum Press, pp. 133–136, 1984.
- [7] S. Even, O. Goldreich, and Y. Yacobi, Electronic Wallet.
 - *Advances in Cryptology: Proceedings of Crypto83*, (D. Chaum editor), Plenum Press, pp. 383–386, 1984.
- [8] S. Even and O. Goldreich, On the Power of Cascade Ciphers.
 - *Advances in Cryptology: Proceedings of Crypto83*, (D. Chaum editor), Plenum Press, pp. 43–50, 1984.
 - *ACM Trans. on Computer Systems*, Vol. 3, No. 2, pp. 108–116, 1985.
- [9] O. Goldreich, On Concurrent Identification Protocols.

- *Advances in Cryptology: Proceedings of Eurocrypt84*, (T. Beth et. al. eds.), Lecture Note in Computer Science (209) Springer Verlag, pp. 387–396, 1985.
- [10] 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.
 - *Jour. of the ACM*, Vol. 33, No. 4, Oct. 1986, pp. 792–807.
- [11] O. Goldreich, Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle is NP-Hard.
- Unpublished manuscript, July 1984.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [12] O. Goldreich and S. Micali. The Weakest Pseudo-Random Generator Implies the Strongest One.
- Unpublished manuscript, October 1984.
- [13] O. Goldreich, On the Number of Monochromatic and Close Beads in a Rosary.
- *Advances in Cryptology: Proceedings of Eurocrypt84*, (T. Beth et. al. eds.), Lecture Note in Computer Science (209) Springer Verlag, pp. 127–141, 1985.
 - *Discrete Mathematics*, Vol. 80, 1990, pp. 59–68.
- [14] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, RSA/Rabin Functions: Certain Parts are As Hard As the Whole.
- *Proc. of the 25th IEEE Symp. on Foundation of Computer Science (FOCS)*, 1984, pp. 449–457.
 - (partial result w/ B. Chor only), *Advances in Cryptology – Crypto ‘84 (Proceedings)*, Lecture Note in Computer Science (196) Springer Verlag, pp. 303–313, 1985.
 - *SIAM J. on Comp.*, Vol. 17, No. 2, April 1988, pp. 194–209.
- [15] O. Goldreich, S. Goldwasser and S. Micali, On the Cryptographic Applications of Random Functions.
- *Advances in Cryptology – Crypto ‘84 (Proceedings)*, (G.R. Blakely et. al. eds.), Lecture Note in Computer Science (196) Springer Verlag, pp. 276–288, 1985.
- [16] B. Chor and O. Goldreich, On the Power of Two-Point Based Sampling.
- *Jour. of Complexity*, Vol 5, 1989, pp. 96–106.
- [17] O. Goldreich and L. Shrira, On the Complexity of Global Computation in the Presence of Link Failures – The Case of a Ring.
- *Proc. of the 5th ACM Symp. on Principles of Distributed Computing (PODC)*, pp. 174–185, 1986.
 - *Distributed Computing*, Vol. 5, 1991, pp. 121–131.

- [18] O. Goldreich and L. Shrira, Electing a Leader in a Ring with Link Failures.
- *ACTA Informatica*, Vol. 24, pp. 79–91, 1987.
- [19] 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.
 - *SIAM J. on Comp.*, Vol. 17, No. 2, April 1988, pp. 230–261.
- [20] 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.
- [21] B. Chor and O. Goldreich, An Improved Parallel Algorithm for Integer GCD.
- *Algorithmica*, 5, pp. 1–10, 1990.
- [22] 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.
 - *IEEE Trans. on Inform. Theory*, Vol. 36, No. 1, pp. 40–46, Jan. 1990.
- [23] S. Even, O. Goldreich and A. Shamir, On the Security of Ping-Pong Protocols when Implemented Using the RSA.
- *Advances in Cryptology – Crypto ‘85 (Proceedings)*, (H.C. Williams ed.), Lecture Note in Computer Science (218) Springer Verlag, pp. 58–72, 1986.
- [24] B. Chor, O. Goldreich and S. Goldwasser, The Bit Security of Modular Squaring given Partial Factorization of the Modulus.
- *Advances in Cryptology – Crypto ‘85 (Proceedings)*, (H.C. Williams ed.), Lecture Note in Computer Science (218) Springer Verlag, pp. 448–457, 1986.
- [25] O. Goldreich, Two Remarks Concerning the GMR Signature Scheme.
- *Advances in Cryptology – Crypto ‘86 (Proceedings)*, (A.M. Odlyzko ed.), Lecture Note in Computer Science (263) Springer Verlag, pp. 104–110, 1987.
- [26] O. Goldreich, S. Micali, and A. Wigderson, Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs.
- *Proc. of the 27th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 174–187, 1986.
 - *Jour. of the ACM*, Vol. 38, No. 3, July 1991, pp. 691–729.
- [27] 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.
 - Journal version with R. Ostrovsky (“Software Protection and Simulation on Oblivious RAMs”) *JACM*, Vol. 43, No. 3, 1996, pp. 431–473.
- [28] 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.
- [29] Ben-Or, M., O. Goldreich, S. Goldwasser, J. Hastad, J. Kilian, S. Micali, and P. Rogaway, Everything Provable is Provable in Zero-Knowledge.
- *Advances in Cryptology – Crypto ‘88 (Proceedings)*, Lecture Note in Computer Science (403) Springer Verlag, pp. 37–56, 1990.
- [30] R. Bar-Yehuda, O. Goldreich, A. Itai, On the Time-Complexity of Broadcast in Radio Networks: An Exponential Gap Between Determinism and Randomization.
- *Proc. of the 6th ACM Symp. on Principles of Distributed Computing (PODC)*, 1987, pp. 98–108.
 - *Journal of Computer and system Sciences*, Vol. 45, (1992), pp. 104–126.
- [31] 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.
- [32] O. Goldreich and R. Vainish, How to Solve any Protocol Problem – An Efficiency Improvement.
- *Advances in Cryptology – Crypto ‘87 (Proceedings)*, (C. Pomerance ed.), Lecture Note in Computer Science (293) Springer Verlag, pp. 73–86, 1988.
- [33] M. Furer, O. Goldreich, Y. Mansour, M. Sipser, and S. Zachos, On Completeness and Soundness in Interactive Proof Systems.
- *Proc. of the 28th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 449-461, 1987.
 - *Advances in Computing Research: a research annual*, Vol. 5 (Randomness and Computation, S. Micali, ed.), pp. 429–442, 1989.
- [34] 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.
- [35] O. Goldreich and Y. Oren, Definitions and Properties of Zero-Knowledge Proof Systems.
- *Journal of Cryptology*, Vol. 7, No. 1 (1994), pp. 1–32.
- [36] 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.

- *SIAM J. on Computing*, Vol. 22-6 (Dec. 1993), pp. 1163–1175.
- [37] Goldreich, O., and E. Kushilevitz, A Perfect Zero-Knowledge Proof for a Decision Problem Equivalent to Discrete Logarithm.
- *Advances in Cryptology – Crypto ‘88 (Proceedings)*, Lecture Note in Computer Science (403) Springer Verlag, pp. 57–70, 1990.
 - *Journal of Cryptology*, Vol. 6, No. 2, (1993), pp. 97–116.
- [38] 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.
 - *Journal of Cryptology*, Vol. 9, No. 1, 1996, pp. 35–67.
- [39] 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.
- [40] 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.
 - *Journal of Computer and system Sciences*, Vol. 44, No. 2, April 1992, pp. 193–219.
- [41] 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.
- [42] 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.
 - *SIAM Journal on Computing*, Vol. 25, No. 1, February 1996, pp. 169–192.
- [43] O. Goldreich, A Note on Computational Indistinguishability.
- *IPL*, Vol. 34, pp. 277–281, May 1990.
- [44] O. Goldreich and E. Petrank, Quantifying Knowledge Complexity.
- *Proc. of the 32nd IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 59–68, 1991.
 - *Computational Complexity*, Vol. 8, pages 50–98, 1999.
- [45] 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.
 - *Random Structures and Algorithms*, Vol. 3, No. 2, (1992), pp. 163–174.

- [46] 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.
- [47] O. Goldreich, A. Herzberg, and Y. Mansour, Source to Destination Communication in the Presence of Faults.
- *Proc. of the 8th ACM Symp. on Principles of Distributed Computing (PODC)*, 1989, pp. 85–102.
- [48] O. Goldreich, A Uniform Complexity Treatment of Encryption and Zero-Knowledge.
- *Journal of Cryptology*, Vol. 6, No. 1, (1993), pp. 21–53.
- [49] B. Awerbuch, O. Goldreich, and A. Herzberg, A Quantitative Approach to Dynamic Networks.
- *Proc. of the 9th ACM Symp. on Principles of Distributed Computing (PODC)*, pp. 189–204, 1990.
- [50] 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.
- [51] 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.
 - *Journal of Random structures and Algorithms*, Vol. 3, No. 3, (1992), pp. 289–304.
- [52] 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.
 - *Computational Complexity*, Vol. 3 (1993), pp. 141–167.
- [53] 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.
 - *Computational Complexity*, Vol. 4, No. 4 (1993), pp. 319–354.
- [54] 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.
- [55] 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.
 - *SIAM J. on Computing*, Volume 27, Number 2, April 1998, Pages 506–544.
- [56] 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.
 - *Random Structures and Algorithms*, Vol. 13, No. 1, pp. 1–16, Aug. 1998.
- [57] 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.
- [58] O. Goldreich and D. Sneh, On the Complexity of Global Computation in the Presence of Link Failures: the case of Unidirectional Faults.
- *Proc. of the 11th ACM Symp. on Principles of Distributed Computing (PODC)*, pp. 103–111, 1992.
- [59] 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.
- [60] M. Bellare and O. Goldreich, Proofs of Computational Ability.
- *Theory of Cryptography Library*, record Arc-03.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [61] 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.
- [62] R. Canetti, G. Even, and O. Goldreich, Lower Bounds for Sampling Algorithms for Estimating the Average.
- *IPL*, Vol. 53, pp. 17–25, 1995.
- [63] 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.
 - *Journal of Random structures and Algorithms*, Volume 11, Number 4, December 1997, pages 315–343.
- [64] 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.
 - *SIAM J. on Computing*, Volume 27, Number 4, pp. 1116–1141, August 1998.

- [65] 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.
- [66] O. Goldreich and S. Safra, A Combinatorial Consistency Lemma with application to the PCP Theorem.
- *Random97*, Springer LNCS, Vol. 1269, pp. 67–84.
 - *SIAM J. on Computing*, Volume 29, Number 4, pages 1132–1154, 1999.
- [67] 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.
- [68] O. Goldreich, N. Nisan and A. Wigderson, On Yao’s XOR-Lemma.
- *ECCC*, TR95-050, 1995.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [69] O. Goldreich, L.A. Levin, and N. Nisan, On Constructing 1-1 One-way Functions.
- *ECCC*, TR95-029, 1995.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [70] 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.
- [71] 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.
 - *JACM*, Vol. 45, No. 6, pages 965–982, November 1998.
- [72] M. Bellare, O. Goldreich and M. Sudan, Free Bits, PCPs and Non-Approximability – Towards Tight Results.
- *Proc. of the 36th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 422-431, 1995.
 - *SIAM J. on Computing*, Vol. 27, No. 3, pp. 804–915, June 1998.
- [73] 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.
 - *SIAM J. on Disc. Math.*, Vol. 13, No. 4, pages 535–570, 2000.

- [74] 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.
- [75] 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.
 - *JACM*, pages 653–750, July 1998.
- [76] O. Goldreich and J. Hastad, On the Complexity of Interactive Proofs with Bounded Communication.
- *IPL*, Vol. 67 (4), pages 205–214, 1998.
- [77] O. Goldreich and A. Wigderson, On the Circuit Complexity of Perfect Hashing.
- *ECCC*, TR96-041, 1996.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [78] O. Goldreich and D. Ron, On Universal Learning Algorithms.
- *IPL*, Vol. 63, 1997, pages 131–136.
- [79] O. Goldreich, S. Goldwasser, and S. Halevi, Collision-Free Hashing from Lattice Problems.
- *ECCC*, TR96-042, 1996.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [80] O. Goldreich and D. Ron, Property Testing in Bounded Degree Graphs.
- *Proc. of the 29th ACM Symp. on Theory of Computing (STOC)*, pages 406–415, 1997.
 - *Algorithmica*, Vol. 32 (2), pages 302–343, 2002.
- [81] O. Goldreich, The Graph Clustering Problem has a Perfect Zero-Knowledge Proof.
- *ECCC*, TR96-054, November 1996.
 - Journal version with A. De-Santis, G. Di-Crescenzo, and G. Persiano, *IPL*, Vol. 69, pp. 201–206, 1999.
- [82] O. Goldreich, S. Goldwasser and S. Halevi, Public-Key Cryptosystems from Lattice Reduction Problems.
- Proceedings of *Crypto97*, Springer LNCS, Vol. 1294, pp. 112–131.
- [83] O. Goldreich and B. Meyer, Computational Indistinguishability – Algorithms vs. Circuits.
- *Theoretical Computer Science*, Vol. 191 (1998), pages 215–218.
- [84] S. Decatur, O. Goldreich, and D. Ron, Computational Sample Complexity.
- *10th COLT*, pp. 130–142, 1997.

- *SIAM J. on Computing*, Vol. 29, Nr. 3, pages 854–879, 1999.
- [85] 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.
- [86] 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.
- [87] 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.
- [88] O. Goldreich and D. Zuckerman, Another proof that BPP subseteq PH (and more).
- *ECCC*, TR97-045, 1997.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650, 2011.
- [89] O. Goldreich and M. Sudan, Computational Indistinguishability: A Sample Hierarchy.
- *13th IEEE Conference on Computational Complexity*, pages 24–33, 1998.
 - *JCSS*, Vol. 59, pages 253–269, 1999.
- [90] O. Goldreich and S. Goldwasser, On the Limits of Non-Approximability of Lattice Problems.
- *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 1–9, 1998.
 - *JCSS*, Vol. 60, pages 540–563, 2000.
- [91] O. Goldreich and D. Ron, A Sublinear Bipartiteness Tester for Bounded Degree Graphs.
- *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 289–298, 1998.
 - *Combinatorica*, Vol. 19 (3), pages 335–373, 1999.
- [92] R. Canetti, O. Goldreich and S. Halevi. The Random Oracle Methodology, Revisited.
- *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 209–218, 1998.
 - *Jour. of the ACM*, Vol. 51 (4), pages 557–594, July 2004.
- [93] O. Goldreich, A. Sahai and S. Vadhan, Honest-Verifier Statistical Zero-Knowledge Equals General Statistical Zero-Knowledge.
- *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 399–408, 1998.
- [94] O. Goldreich, S. Goldwasser, E. Lehman and D. Ron, Testing Monotonicity.
- *Proc. of the 39th FOCS*, pages 426–435, 1998.
 - Journal version with A. Samorodnitsky, *Combinatorica*, Vol. 20 (3), pages 301–337, 2000.

- [95] 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.
- [96] 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.
- [97] 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.
- [98] M. Bellare, O. Goldreich and H. Krawczyk, Beyond the Birthday Barrier, Without Counters.
- Proceedings of *Crypto99*, Springer LNCS, Vol. 1666, pages 270–287.
- [99] O. Goldreich, D. Ron, and M. Sudan, Chinese Remaindering with Errors.
- *Proc. of the 31st ACM Symp. on Theory of Computing (STOC)*, pages 225–234, 1999.
 - *IEEE Transactions on Information Theory*, Vol. 46, No. 4, July 2000, pages 1330–1338.
- [100] 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.
- [101] Y. Dodis, O. Goldreich, E. Lehman, S. Raskhodnikova, D. Ron and A. Samorodnitsky, Improved Testing Algorithms for Monotonicity.
- *Random99*, Springer LNCS, Vol. 1671, pages 97–108.
- [102] O. Goldreich and A. Wigderson, Improved Derandomization of BPP using a Hitting Set Generator.
- *Random99*, Springer LNCS, Vol. 1671, pages 131–137.
- [103] O. Goldreich, S. Goldwasser, and S. Micali. Interleaved Zero-Knowledge in the Public-Key Model.
- *ECCC*, TR99-024, 1999.
- [104] 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.
- [105] O. Goldreich, S. Vadhan and A. Wigderson, Simplified Derandomization of BPP using a Hitting Set Generator.
- *ECCC*, TR00-004, 2000.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650, 2011.

- [106] O. Goldreich and A. Wigderson, On Pseudorandomness with respect to Deterministic Observers.
- *Random00, ICALP workshops 2000*, Carleton Scientific (Proc. in Inform. 8), pages 77–84.
- [107] O. Goldreich and D. Ron, On Testing Expansion in Bounded-Degree Graphs.
- *ECCC*, TR00-020, 2000.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650, 2011.
- [108] O. Goldreich and Y. Lindell, Session-Key Generation using Human Passwords Only.
- Proceedings of *Crypto01*, pages 408–432.
 - *Jour. of Cryptology*, pages 241–340, Summer 2006.
- [109] O. Goldreich, Candidate One-Way Functions Based on Expander Graphs.
- *Cryptology ePrint Archive*, Report 2000/063, 2000.
 - *ECCC*, TR00-090, 2000.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650, 2011.
- [110] O. Goldreich and V. Rosen, On the Security of Modular Exponentiation with Application to the Construction of Pseudorandom Generators.
- *Journal of Cryptology*, Vol. 16, pages 71–93, 2003.
- [111] 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.
 - *Journal of ACM*, Vol. 59, No. 2, Art. 6, April 2012.
- [112] O. Goldreich and L. Trevisan, Three Theorems regarding Testing Graph Properties.
- Proceedings of *42nd FOCS*, pages 460–469, 2001.
 - *Random Structures and Algorithms*, Vol. 23 (1), pages 23–57, August 2003.
- [113] O. Goldreich, S. Vadhan and A. Wigderson, On interactive proofs with a laconic provers.
- Proceedings of *28th ICALP*, Springer’s LNCS 2076, pages 334–345, 2001.
 - *Computational Complexity*, Vol. 11, pages 1–53, 2002.
- [114] B. Barak, O. Goldreich, S. Goldwasser and Y. Lindell, Resetably-Sound Zero-Knowledge and its Applications.
- Proceedings of *42nd FOCS*, pages 116–125, 2001.
- [115] O. Goldreich, H. Karloff, L. Schulman and L. Trevisan, Lower Bounds for Linear Locally Decodable Codes and Private Information Retrieval.
- Proceedings of *17th IEEE Conference on Computational Complexity*, pages 175–183, 2002.

- *Computational Complexity*, Vol. 15, No. 3, Pages 263–296, October 2006.
- [116] O. Goldreich, Concurrent Zero-Knowledge With Timing, Revisited.
- *Proc. of the 34th STOC*, pages 332–340, 2002.
 - In *Theoretical Computer Science: Essays in memory of Shimon Even*, Springer, LNCS Festschrift, Vol. 3895, pages 27–87, 2006.
- [117] B. Barak and O. Goldreich, Universal arguments and their applications.
- Proceedings of *17th Conference on Computational Complexity*, pages 194–203, 2002.
 - *SIAM J. on Computing*, Volume 38, Issue 5, pages 1661–1694, 2008.
- [118] O. Goldreich, Using the FGLSS-reduction to Prove Inapproximability Results for Minimum Vertex Cover in Hypergraphs.
- *ECCC*, TR01-102, 2001.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650, 2011.
- [119] O. Goldreich, Y. Lustig and M. Naor, On Chosen Ciphertext Security of Multiple Encryptions.
- *Cryptology ePrint Archive*, Report 2002/089, 2002.
- [120] O. Goldreich and M. Sudan, Locally Testable Codes and PCPs of Almost-Linear Length.
- Proceedings of *43rd FOCS*, pages 13–22, 2002.
 - *JACM*, Vol. 53, No. 4, July 2006, pp. 558–655.
- [121] O. Goldreich and A. Wigderson, Derandomization that is rarely wrong from short advice that is typically good.
- Proceedings of *RANDOM*, Springer LNCS, Vol. 2483, pages 209–223, 2002.
- [122] N. Alon, O. Goldreich and Y. Mansour. Almost k -wise independence versus k -wise independence.
- *IPL*, Vol. 88 (3), pages 107–110, 2003.
- [123] O. Goldreich. The GGM Construction does NOT yield Correlation Intractable Function Ensembles.
- *Cryptology ePrint Archive*, Report 2002/110, 2002.
 - *ECCC*, TR02-047, 2002.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650, 2011.
- [124] E. Ben-Sasson, O. Goldreich and M. Sudan. Bounds on 2-Query Codeword Testing.
- Proceedings of *RANDOM*, Springer LNCS, Vol. 2764, pages 216–227, 2003.
- [125] O. Goldreich, S. Goldwasser and A. Nussboim. On the Implementation of Huge Random Objects.
- Proceedings of *44th FOCS*, pages 68–79, 2003.

- *SICOMP*, Vol. 39, No. 7, May 2010.
- [126] R. Canetti, O. Goldreich and S. Halevi. On the random-oracle methodology as applied to length-restricted signature schemes.
- *1st Theory of Cryptography Conference*, Springer LNCS, Vol. 2951, pages 40–57, 2004
- [127] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Robust PCPs of Proximity, Shorter PCPs and Applications to Coding.
- Proceedings of the *36th STOC*, pages 1-10, 2004.
 - *SIAM J. on Computing* (special issue on Randomness and Complexity), Volume 36, Issue 4, pages 889–974, 2006.
- [128] O. Goldreich and D. Ron. On Estimating the Average Degree of a Graph.
- *ECCC*, TR04-013, 2004.
- [129] O. Goldreich, M. Sudan and L. Trevisan. From logarithmic advice to single-bit advice.
- *ECCC*, TR04-093, 2004.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [130] M. Bellare, O. Goldreich and A. Mityagin, The Power of Verification Queries in Message Authentication and Authenticated Encryption.
- Cryptology ePrint Archive, Report 2004/309.
- [131] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. Vadhan. Short PCPs Verifiable in Polylogarithmic Time.
- In the proceedings of *20th IEEE Conference on Computational Complexity*, pages 120–134, 2005.
- [132] O. Goldreich and D. Ron, Approximating Average Parameters of Graphs.
- In the proceedings of *10th RANDOM*, Springer LNCS, Vol. 4110, pages 363–374, 2006.
 - *Random Structures and Algorithms*, Volume 32, Number 3, pages 473–493, 2008.
- [133] 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.
- [134] O. Goldreich, On Expected Probabilistic Polynomial-Time Adversaries: A suggestion for restricted definitions and their benefits.
- Proceedings of the *4th Theory of Cryptography Conference*, Springer LNCS, Vol. 4392, pages 174–193, 2007.
 - *Journal of Cryptology*, Volume 23, Issue 1, pages 1–36, 2010.
- [135] M. Bellare and O. Goldreich, On Probabilistic versus Deterministic Provers in the Definition of Proofs Of Knowledge.

- *ECCC*, TR06-136, 2006.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [136] O. Goldreich and O. Sheffet, On the randomness complexity of property testing.
- Proceedings of *11th RANDOM*, Springer LNCS, Vol. 4627, pages 509–524, 2007.
 - *Computational Complexity*, Volume 19, Number 1, pages 99–133, 2010.
- [137] K. Barhum, O. Goldreich and A. Shraibman, On approximating the average distance between points.
- Proceedings of *11th RANDOM*, Springer LNCS, Vol. 4627, pages 296–310, 2007.
- [138] O. Goldreich, On the Average-Case Complexity of Property Testing.
- *ECCC*, TR07-057, 2007.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [139] O. Goldreich and O. Meir, The Tensor Product of Two Good Codes Is Not Necessarily Robustly Testable.
- *IPL*, Vol. 112, pages 351–355, 2012.
- [140] O. Goldreich and D. Ron, Algorithmic Aspects of Property Testing in the Dense Graphs Model.
- Proceedings of *13th RANDOM*, Springer LNCS, Vol. 5687, pages 520–533, 2009.
 - *SICOMP*, Vol. 40, No. 2, pages 376–445, 2011.
- [141] O. Goldreich and D. Ron, On Proximity Oblivious Testing.
- Proceedings of the *41st STOC*, pages 141–150, 2009.
 - *SICOMP*, Vol. 40, No. 2, pages 534–566, 2011.
- [142] O. Goldreich, M. Krivelevich, I. Newman, and E. Rozenberg, Hierarchy Theorems for Property Testing.
- Proceedings of *13th RANDOM*, Springer LNCS, Vol. 5687, pages 504–519, 2009.
 - *Computational Complexity*, Vol. 21 (1), pages 129–192, 2012.
- [143] Z. Brakerski and O. Goldreich, From absolute distinguishability to positive distinguishability.
- *ECCC*, Report TR09-031, Apr. 2009
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [144] O. Goldreich, A Candidate Counterexample to the Easy Cylinders Conjecture.
- *ECCC*, Report TR09-028, Apr. 2009
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650 , 2011.
- [145] O. Goldreich, B. Juba, and M. Sudan, A Theory of Goal-Oriented Communication.
- *Journal of ACM*, Vol. 59, No. 2, Art. 8, April 2012.

- [146] D. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev, More Constructions of Lossy and Correlation-Secure Trapdoor Functions.
- Proceedings of *13th PKC*, Springer LNCS, Vol. 6056, pages 279–295, 2010.
 - *Journal of Crypto.*, Online First, 10-Nov-2011.
- [147] L. Avigad and O. Goldreich, Testing Graph Blow-Up.
- Proceedings of *15th RANDOM*, Springer LNCS, Vol. 6845, pages 389–399, 2011.
- [148] O. Goldreich and T. Kaufman. Proximity Oblivious Testing and the Role of Invariances.
- Proceedings of *15th RANDOM*, Springer LNCS, Vol. 6845, pages 579–592, 2011.
- [149] A. Czumaj, O. Goldreich, D. Ron, C. Seshadhri, A. Shapira, and C. Sohler, Finding Cycles and Trees in Sublinear Time.
- [150] O. Goldreich. On Testing Computability by Small Width OBDDs.
- Proceedings of *14th RANDOM*, Springer LNCS, Vol. 6302, pages 574–586, 2010.
- [151] O. Goldreich. In a World of $P=BPP$.
- ECCC TR10-135, 2010.
 - In *Studies in Complexity and Cryptography*, Pringer, LNCS, Vol. 6650, 2011.
- [152] O. Goldreich and O. Meir. Input-Oblivious Proof Systems and a Uniform Complexity Perspective on $P/poly$.
- ECCC TR11-023, 2011.
- [153] O. Goldreich. Two Comments on Targeted Canonical Derandomizers.
- ECCC TR11-047, 2011.
- [154] O. Goldreich and R. Rothblum, Enhancements of Trapdoor Permutations.
- *Journal of Cryptology*, Online First, 12-Sept-2012.
- [155] O. Goldreich and R. Izsak. Monotone Circuits: One-Way Functions versus Pseudorandom Generators.
- *ToC*, Vol. 8, Art. 10, pages 231–238, 2012.
- [156] O. Goldreich. On the Effect of the Proximity Parameter on Property Testers.
- ECCC TR12-012, 2012.
- [157] O. Goldreich and I. Shinkar. Two-Sided Error Proximity Oblivious Testing.
- Proceedings of *16th RANDOM*, Springer LNCS, Vol. 7408, pages 565–578, 2012.
- [158] 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.
- [159] O. Goldreich and A. Wigderson. On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions.
- ECCC TR13-043, 2013.
- [160] O. Goldreich. On Multiple Input Problems in Property Testing.
- ECCC TR13-067, 2013.
- [161] O. Goldreich. On the Communication Complexity Methodology for Proving Lower Bounds on the Query Complexity of Property Testing.
- ECCC TR13-073, 2013.
- [162] O. Goldreich and D. Ron. On Sample-Based Testers.
- ECCC TR13-109, 2013.
- [163] O. Goldreich and A. Wigderson. On Derandomizing Algorithms that Err Extremely Rarely.
- ECCC TR13-152, 2013.