List of Publications

Oded Goldreich

April 11, 1997

1 Theses

- "On the Complexity of Some Edge Testing Problems", M.Sc. thesis, Computer Science Dept., Technion, Haifa, Israel. Thesis adviser: Prof. S. Even, 1982.
- "On the Security of Cryptographic Protocols and Cryptosystems", D.Sc. thesis, Computer Science Dept., Technion, Haifa, Israel. Thesis adviser: Prof. S. Even, 1983.

2 Original Papers in Refereed Journals

Published

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

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

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

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

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

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

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

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

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

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

[J11] M. Furer, O. Goldreich, Y. Mansour, M. Sipser, and S. Zachos, "On Completeness and Soundness in Interactive Proof Systems", *Advances in Computing Research: a research annual*, Vol. 5 (Randomness and Computation, S. Micali, ed.), pp. 429–442, 1989.

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

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

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

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

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

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

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

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

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

[J21] S. Ben-David, B. Chor, O. Goldreich, and M. Luby, "On the Theory of Average Case Complexity", *Journal of Computer and system Sciences*, Vol. 44, N0. 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] Goldreich, O., 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.

Accepted

[J37] O. Goldreich, S. Goldwasser, and N. Linial, "Fault-tolerant Computations without Assumptions: the Two-party Case", *SIAM J. on Computing*, May 1994

[J38] O. Goldreich, R. Ostrovsky and E. Petrank, "Knowledge Complexity and Computational Complexity", *SICOMP*, editor's letter of Dec. 1995.

[J39] 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*, editor's email Dec. 5, 1996.

[J40] M. Bellare, O. Goldreich and M. Sudan, "Free Bits and Non-Approximability", *SICOMP*, editor's letter Dec. 17, 1996.

Submitted

[J41] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, "Private Information Retrieval", submitted to *Journal of the ACM*, Jan. 1996.

[J42] O. Goldreich and J. Hastad, "On the Message Complexity of Interactive Proof Systems", submitted to *IPL*, March 1996.

[J43] O. Goldreich and E. Petrank, "Quantifying Knowledge Complexity", submitted to *Computational Complexity*, July 1996,

[J44] O. Goldreich and A. Wigderson, On the Circuit Complexity of Perfect Hashing, submitted to IPL, July 24, 1996.

[J45] O. Goldreich, S. Goldwasser and D. Ron, Property Testing and its connection to Learning and Approximation, submitted to *Journal of the ACM*, Oct. 1996.

[J46] O. Goldreich and B. Meyer, "Computational Indistinguishability – Algorithms vs. Circuits", submitted to TCS, Dec. 1996.

[J47] O. Goldreich and D. Ron, "On Universal Learning Algorithms", submitted to IPL, Jan. 14, 1997.

[J48] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Veličković, "Approximations of General Independent Distributions", submitted to RS&A, Feb. 16, 1997.

3 Original Papers in (Refereed) Conference Proceedings

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[C19] O. Goldreich, S. Goldwasser, and N. Linial, "Fault-tolerant Computations without Assumptions: the Two-party Case", *Proc. of the 32nd IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 447–457, 1991. (This is an extended abstract of No. J37.)

[C20] O. Goldreich, and E. Petrank, "Quantifying Knowledge Complexity", *Proc. of the 32nd IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 59–68, 1991. (This is an extended abstract of No. J43.)

[C21] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Veličković, "Approximations of General Independent Distributions", *Proc. of the 24th ACM Symp. on Theory of Computing (STOC)*, pp. 10–16, 1992. (This is an extended abstract of No. J48.)

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

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

[C24] O. Goldreich and A. Wigderson, "Tiny Families of Functions with Random Properties: A Quality–Size Trade–off for Hashing", *Proc. of the 26th ACM Symp. on Theory of Computing (STOC)*, pp. 574-583, 1994. (This is an extended abstract of No. J39.)

[C25] O. Goldreich, R. Ostrovsky and E. Petrank, "Knowledge Complexity and Computational Complexity", *Proc. of the 26th ACM Symp. on Theory of Computing (STOC)*, pp. 534-543, 1994. (This is an extended abstract of No. J38.)

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

[C27] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, "Private Information Retrieval", *Proc. of the 36th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 41-50, 1995. (This is an extended abstract of No. J41.)

[C28] M. Bellare, O. Goldreich and M. Sudan, "Free Bits and Non-Approximability", *Proc. of the 36th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 422-431, 1995. (This is an extended abstract of No. J40.)

[C29] O. Goldreich, R. Rubinfeld and M. Sudan, "Learning polynomials with queries: the highly noisy case", *Proc. of the 36th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 294-303, 1995.

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

[C31] O. Goldreich, S. Goldwasser and D. Ron, Property Testing and its connection to Learning and Approximation, *Proc. of the 37th IEEE Symp. on Foundation of Computer Science (FOCS)*, pp. 339–348, 1996. (This is an extended abstract of No. J45.)

[C32] O. Goldreich and D. Ron, Property Testing in Bounded Degree Graphs, *Proc. of the 29th ACM Symp. on Theory of Computing (STOC)*, 1997.

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

[C33] 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.)

[C34] S. Even and O. Goldreich, "On The Security of Multi-Party Ping-Pong Protocols", in *Advances in Cryptology: Proceedings of Crypto82*, (D. Chaum et al. editors), Plenum Press, p. 315, 1983. (This is an abstract of No. C1.)

[C35] 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.)

[C36] O. Goldreich, "A Simple Protocol for Signing Contracts", in *Advances in Cryptology: Proceedings of Crypto83*, (D. Chaum editor), Plenum Press, pp. 133–136, 1984.

[C37] 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.

[C38] S. Even, O. Goldreich, and Y. Yacobi, "Electronic Wallet", in *1984 International Zurich Seminar on Digital Communication*, IEEE Cat. No. 84CH1998-4, pp. 199–201, March 1984. (This is an extended abstract of No. C37.)

[C39] 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.

[C40] 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.

[C41] 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.

[C42] 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.

[C43] 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.

[C44] 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.

[C45] 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.)

[C46] 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.

[C47] 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.)

[C48] O. Goldreich, "Towards a Theory of Software Protection", in *Advances in Cryptology – Crypto '86 (Proceedings)*, (A.M. Odlyzko ed.), Lecture Note in Computer Science (263) Springer Verlag, pp. 426–439, 1987. (This is a preliminary version of No. C8.)

[C49] 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.)

[C50] O. Goldreich and S. Micali, "Zero Knowledge and the Design of Secure Protocols", appeared in the proceedings of *Globecom87*, 1987.

[C51] 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.

[C52] 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.)

[C53] 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.

[C54] 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.)

[C55] 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.)

[C56] S. Ben-David, B. Chor, O. Goldreich, and M. Luby, "On the Theory of Average Case Complexity". *Proc. of the 4th conf. on Structure in Complexity Theory*, (This is an abstract of No. C13.)

[C57] 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.)

[C58] 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.

[C59] 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.)

[C60] 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.)

[C61] 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.

[C62] 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.

[C63] 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.

[C64] 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.

[C65] 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.

[C66] S. Decatur, O. Goldreich, and D. Ron, "Computational Sample Complexity", to appear in *COLT*, 1997.

[C67] O. Goldreich and S. Safra, "A Combinatorial Consistency Lemma with application to the PCP Theorem", to appear in *Random97*,

4 Survey Papers

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

[S2] "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.

[S3] "What is an Envelope", *Almost 2000* (a popular journal for Science and Technology), Vol. 1, pp. 15–17, 1994, (in Hebrew).

[S4] "Probabilistic Proof Systems", *Proceedings of the International Congress of Mathematicians 1994*, Birkhäuser Verlag, Basel, 1995, pp. 1395–1406.

[S5] "On Yao's XOR-Lemma", *ECCC*, TR95-050, 1995. (With N. Nisan and A. Wigderson.)

[S6] "Three XOR-Lemmas – An Exposition", *ECCC*, TR95-056, 1995.

[S7] "A Taxonomy of Proof Systems", to appear in *Complexity Theory Retrospective II*, L.A. Hemaspaandra and A. Selman (eds.), 1997. (This is a revision of No. S2.)

5 Class Notes and Books

[B1] "Foundations of Cryptography – Class Notes", Computer Science Department, Technion, Spring 1989, 184 pages.

[B2] "Theory of Computation", Computer Science Dept., Technion, Spring 1989, 184 pages, in Hebrew. (Third edition: Feb. 1992).

[B3] "Foundations of Cryptography – Fragments of a Book", Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, February 1995, 292 pages.

6 Other Work

Papers in Electronic Forum (unrefereed)

[O1] O. Goldreich, L.A. Levin, and N. Nisan, "On Constructing 1-1 One-way Functions", *ECCC*, TR95-029, 1995.

[O2] O. Goldreich and D. Ron, "On Universal Learning Algorithms", *eCOLT*, TR96-008, July 1996. (See J47.)

[O3] O. Goldreich and A. Wigderson, On the Circuit Complexity of Perfect Hashing, *ECCC*, TR96-041, 1996. (See J44.)

[O4] O. Goldreich, S. Goldwasser, and S. Halevi, Collision-Free Hashing from Lattice Problems, *ECCC*, TR95-042, 1996.

[O5] O. Goldreich and S. Safra, "A Combinatorial Consistency Lemma with application to the PCP Theorem", *ECCC*, TR96-047, 1996.

[O6] O. Goldreich, "The Graph Clustering Problem has a Perfect Zero-Knowledge Proof", *ECCC*, TR96-054, November 1996.

[O7] O. Goldreich, S. Goldwasser and S. Halevi, "Public-Key Cryptosystems from Lattice Reduction Problems", TR96-056, November 1996.

[O8] O. Goldreich and B. Meyer, "Computational Indistinguishability – Algorithms vs. Circuits", *ECCC*, TR96-067, 1996. (See J46.)

Research Reports (which did not appear elsewhere)

[O9] "Graph Partition into Equinumerous Connected Components is NP-Complete", TR No. 202, Computer Science Dept., Technion, Haifa, Israel, 1981.

[O10] "A Protocol for Sending Certified Mail", TR No. 239, Computer Science Dept., Technion, Haifa, Israel, 1982.

[O11] "On the Power of non-binary Block-Ciphers", TR No. 264, Computer Science Dept., Technion, Haifa, Israel, 1983.

[O12] "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)

[O13] "Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle is NP-Hard", July 1984.

[O14] "The Weakest Pseudo-Random Generator Implies the Strongest One", October 1984, (with S. Micali).

[O15] "Finding a Second Solution is NP-Complete for Almost All Known NPC Problems", May 1986, (with Y. Moses).