Curriculum Vitae

Oded Goldreich

January 3, 2019

Current Position: Professor of Computer Science, Weizmann Institute of Science, Rehovot, Israel. Incumbent of the Meyer W. Weisgal Professorial Chair.

Personal Data: Born in Israel on February 4th, 1957. Married to Dana Ron.

Citizenship: Israeli. Passport number 20663357.

Research Interests and Expertise:

- Main current focus: Randomness and Computation.
  In particular, Property Testing, Pseudorandomness, and Probabilistic Proof Systems.
- Additional interest: Complexity Theory.
- Past expertise: Foundations of Cryptography.
- Additional past interest: Distributed Computation.

Degrees

B.A. in Computer Science (*Cum Laude*), Technion, Israel. October 1977 through June 1980.

M.Sc. in Computer Science, Technion, Israel. October 1980 through February 1982. Thesis adviser: Prof. S. Even. Thesis Title: "On the Complexity of Some Edge Testing Problems".

D.Sc. in Computer Science, Technion, Israel. March 1982 through June 1983. Thesis adviser: Prof. S. Even. Thesis Title: "On the Security of Cryptographic Protocols and Cryptosystems".

Contents

1 Research Contributions

My field of research is the theory of computation. I have worked mostly on a variety of subjects related to randomized computations (e.g., *pseudorandom generators*, *probabilistic proof systems*, and *property testing*) and to cryptography (e.g., *zero-knowledge* and *secure multi-party computation*). These areas are somewhat overlapping; for example, pseudorandomness and zero-knowledge are relevant both to randomized computations and to cryptography. Some of my contributions to these areas are

- Showing *how to construct zero-knowledge proof systems for any language in NP*, using any commitment scheme [26].
- Showing *how to solve any multi-party protocol problem*, using any trapdoor permutation [28].
- Presenting a generic *hardcore predicate for any one-way function* [39].
- Showing *how to construct pseudorandom functions* from any pseudorandom generators [10].
- Initiating a systematic study of *propery testing* [75], and advancing its developement in subsequent works (e.g., [80, 91, 94, 141]).
- Studying numerous aspects of the foundations of cryptography, pseudorandomness, zero-knowledge proofs, interactive proofs, and probabilistically checkable proofs (PCPs). Specific contributions include
  - Constructing *randomness extractors* (e.g., [19]) and *small sample spaces* (e.g., [16, 51, 56]).
  - Advancing the study of *probabilistically checkable proofs* (e.g., by the introduction of the Long-Code [72] and PCPs of Proximity [127]).
  - Initiating a systematic study of locally testable codes [120] and introducing Private Information Retrieval [71].

I also have research experience in the area of *distributed computing* and in other areas of the theory of computation.

Works and Publications

A full list of all my research articles and monographs follows. An annotated list is available from my webpage (see `http://www.wisdom.weizmann.ac.il/~oded/pub.html`).

[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*, Springer, 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*, Springer, 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*, Springer, 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*, Springer, 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*, Springer, 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*, Springer, 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*, Springer, 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 Bipartitness 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 Monotinicity.

- *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*, Springer, 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*, Springer, 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*, Springer, 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, Resettably-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*, Springer, 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*, Springer, 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*, Springer, 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*, Springer, 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*, Springer, 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*, Springer, 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*, Springer, 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.

- *RS&A*, Vol. 45, Nr. 2, pages 139–184, 2014.

[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*, Springer, LNCS, Vol. 6650 , 2011.

[152] O. Goldreich and O. Meir. Input-Oblivious Proof Systems and a Uniform Complexity Perspective on P/poly.

- *TOCT*, Vol. 7(4), Art. 16, 2015.

[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.
- *Random Structures and Algorithms*, Vol. 48 (2), pages 341–383, 2016.

[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.

- Proceedings of *18th RANDOM*, 2014.

[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.

- Proceedings of *6th ITCS*, pages 337–345, 2015.
- *TOCT*, Vol. 8(2), 2016.

[163] O. Goldreich and A. Wigderson. On Derandomizing Algorithms that Err Extremely Rarely.

- Proceedings of *46th STOC*, pages 109–118, 2014.

[164] 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.

[165] O. Goldreich and D. Ron. On Learning and Testing Dynamic Environments.

- Proceedings of *55th FOCS*, pages 336–343, 2014.
- *JACM*, Vol. 64 (3), pages 21:1–21:90, 2017.

[166] O. Goldreich and L. Teichner. Super-Perfect Zero-Knowledge Proofs.

- ECCC TR14-097, 2014.

[167] O. Goldreich, E. Viola, and A. Wigderson. On Randomness Extraction in AC0.

- Proceedings of *30th Conference on Computational Complexity*, pages 601–668, 2015.

[168] 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.
- *Inform. and Comput.*, Vol. 261 (Part 2), pages 175–201, 2018.

[169] O. Goldreich and A. Tal. Matrix Rigidity of Random Toeplitz Matrices.

- In *48th STOC*, pages 91–104, 2016.
- *Computational Complexity*, Vol. 27 (2), pages 305–350, 2018.

[170] O. Goldreich. The uniform distribution is complete with respect to testing identity to a fixed distribution.

- ECCC TR16-015, 2016

[171] O. Goldreich and T. Gur. Universal Locally Testable Codes.

- *CJTCS*, Vol. 2018, Art. 3.

[172] O. Goldreich and M. Leshkowitz. On Emulating Interactive Proofs with Public Coins.

- ECCC TR16-066, 2016.

[173] O. Goldreich. Reducing testing affine spaces to testing linearity.

- ECCC TR16-080, 2016

[174] O. Goldreich. Deconstructing 1-local expanders.

- ECCC TR16-152, 2016

[175] O. Goldreich and T. Gur. Universal Locally Verifiable Codes and 3-Round Interactive Proofs of Proximity for CSP.

- ECCC TR16-192, 2016

[176] 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.

[177] O. Goldreich and G. Rothblum. Worst-case to Average-case reductions for subclasses of P.

- ECCC TR17-130, 2017

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

- ECCC TR17-193, 2017

[179] O. Goldreich and D. Ron. The Subgraph Testing Model.

- ECCC TR18-045, 2018.

[180] 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.

[181] I. Dinur, O. Goldreich, and T. Gur. Every set in P is strongly testable under a suitable encoding.

- ECCC TR18-050, 2018.

[182] O. Goldreich and G. Rothblum. Constant-round interactive proof systems for AC0[2] and NC1.

- ECCC TR18-069, 2018.

[183] O. Goldreich. Hierarchy Theorems for Testing Properties in Size-Oblivious Query Complexity.

- ECCC TR18-098, 2018.

[184] O. Goldreich. Flexible models for testing graph properties.

- ECCC TR18-104, 2018.

[185] O. Goldreich. Testing Graphs in Vertex-Distribution-Free Models.

- ECCC TR18-171, 2018.

2 Expository Contributions

In my opinion, the generation of scientific knowledge is of little value if not coupled with the effective dissemination of this knowledge. This calls not only for clear exposition of research contributions but also for the presentation of wider perspectives in surveys, lecture notes and books. In view of these opinions, I am devoting significant portions of my time to the writing of such expositions.

2.1 Books and Lecture Notes

The distinction below is between complete texts that were carefully written and partial texts (which in some cases were written rather casually).

Books (partial preliminary drafts are available from my web-page):

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

The interplay between randomness and computation is one of the most fascinating scientific phenomena uncovered in the last couple of decades. This interplay is at the heart of modern cryptography and plays a fundamental role in complexity theory at large. Specifically, the

interplay of randomness and computation is pivotal to several intriguing notions of probabilistic proof systems and is the focal of the computational approach to randomness. This book provides an introduction to these three, somewhat interwoven domains.

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

This is the first volume of a two-volume work aimed at presenting firm foundations for cryptography; that is, presenting the paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural "security concerns" as well as some of the fundamental results obtained using them. The emphasis is on the clarification of fundamental concepts and on demonstrating the feasibility of solving several central cryptographic problems. This volume focuses on computational difficulty (i.e., one-way functions), pseudorandom generators and zero-knowledge proofs.

[B3] Foundations of Cryptography – Basic Applications, *Cambridge University Press*, 2004.

This is the second volume of a two-volume work aimed at presenting firm foundations for cryptography. In continuation to [B2], this volume treats encryption schemes, signature schemes and general cryptographic protocols. Significant portions of this volume provide expositions that were not published (in any form) before.

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

This book is rooted in the thesis that complexity theory is extremely rich in conceptual content, and that this contents should be explicitly communicated in expositions and courses on the subject. It focuses on several sub-areas of complexity theory, starting from the intuitive questions addresses by the sub-area. The exposition discusses the fundamental importance of these questions, the choices made in the actual formulation of these questions and notions, the approaches that underly the answers, and the ideas that are embedded in these answers.

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

The focus of this book is on the P-vs-NP Question, which is the most fundamental question of computer science, and on the theory of NP-completeness, which is its most influential theoretical discovery. The book also provides adequate preliminaries regarding computational problems and computational models.

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

This book surveys the (complexity-based) theory of pseudorandomness, which emerges from the postulate that a distribution is pseudorandom if it cannot be told apart from the uniform distribution by any efficient procedure.

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

Provides an introduction to Property Testing, which is the study of super-fast algorithms for distinguishing between objects having a predetermined property and objects that are far from having this property. Such approximate decisions aim at unveiling global structural features of huge amounts of data.

Lecture Notes (mostly available from my web-page):

[N8] "Foundations of Cryptography – Class Notes", Computer Science Dept., Technion, Spring 1989, 184 pages.

(Written by students attending my course. Superseeded by [B2] and [B3].)

[N9] "Theory of Computation", Computer Science Dept., Technion, Spring 1989, 184 pages, in Hebrew. (Third edition: Feb. 1992.)

(Undergraduate textbook in Hebrew. Available from my web-page.)

[N10] "Foundations of Cryptography – Fragments of a Book", Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, February 1995, 292 pages.

(A very preliminary draft of [B2]. Available from my web-page.)

[N11] "Introduction to Complexity Theory – Lecture Notes" (for a two-semester course), Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, July 1999, 353 pages.

(Written by students attending my course. Most of the material is presented better in [N13]. Available from my web-page.)

[N12] "Randomized Methods in Computation – Lecture Notes", Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, July 2001, 155 pages.

(Written by students attending my course. The course focused on some of the randomized methods being employed in the study of computation. Available from my web-page.)

[N13] "Introduction to Complexity Theory – Lecture Notes" (for a one-semester course), Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, July 2002, 104 pages.

(Covers less than [N11] and superseeded by [B4]. Available from my web-page.)

2.2 Survey articles

Most of the following surveys attempt to provide high-level presentation of research areas whereas others provide more technical exposition of a single problem or even a single work.

High-level surveys of areas:

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

[S3] "Probabilistic Proof Systems", *Proceedings of the International Congress of Mathematicians 1994*, Birkhäuser Verlag, Basel, 1995, pp. 1395–1406.

[S4] "A Taxonomy of Proof Systems", in *Complexity Theory Retrospective II*, L.A. Hemaspaandra and A. Selman (eds.), Springer, 1997. Pages 109–134.

A preliminary version has appeared 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.

[S5] "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.

[S6] "Combinatorial Property Testing – A Survey", in *DIMACS Series in Disc. Math. and Theoretical Computer Science*, Vol. 43 (Randomization Methods in Algorithm Design), pp. 45–59, 1998.

[S7] "Fundamentals of Cryptography" (Chap. 97.2), in *The Electrical Engineering Handbook*, CRC Press, 2000.

[S8] "Pseudorandomness", in *Notices of AMS*, pages 1209–1216, November 1999.

Extended version in the *Proc. of 27th ICALP*, Springer LNCS, Vol. 1853, pages 687–704, 2000.

[S9] "Computational Complexity", in *Mathematics Unlimited – 2001 and Beyond*, Springer, Pages 507–524.

[S10] "Pseudorandomness – Part I", in *IAS/Park City Mathematics Series*, Vol. 10, 2000.

[S11] "Property Testing in Massive Graphs", in *Handbook of Massive Data Sets*, Kluwer, 2002. Pages 123–147.

[S12] "Cryptography and Cryptographic Protocols", in *PODC Jubilee Issue of Distributed Computing*, Vol. 16, No. 2–3, pages 177–199, 2003.

[S13] "Short Locally Testable Codes and Proofs (Survey)", in *Property Testing*, Springer's LNCS, Vol 6390, 2010.

Superseeds a prior version in *ECCC*, TR05-014, January 2005.

[S14] "Foundations of Cryptography – A Primer", in *Foundations and Trends in Theoretical Computer Science*, Volume 1, Issue 1, 2005.

[S15] "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.

[S16] "Randomness and Computation", in *Handbook of Probability Theory with Applications*, Sage Publishers, 2008.

[S17] "Computational Complexity" (with A. Wigderson), in *The Princeton Companion to Mathematics*, Princeton University Press, 2008.

[S18] "Probabilistic Proof Systems – A Primer", in *Foundations and Trends in Theoretical Computer Science*, Volume 3, Issue 1, 2007.

[S19] "Introduction to Testing Graph Properties", in *Property Testing*, Springer's LNCS, Vol 6390, 2010.

[S20] "A Brief Introduction to Property Testing", in *Property Testing*, Springer's LNCS, Vol 6390, 2010.

[S21] "On the complexity of computational problems regarding distributions" (with S. Vadhan), ECCC, TR11-004.

[S22] "Invitation to Complexity Theory", *XRDS*, Vol. 18, No. 3, Spring 2012.

[S23] "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.

[S24] "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.

[S25] "On Doubly-Efficient Interactive Proof Systems" in *Foundations and Trends in Theoretical Computer Science*, Volume 13, Issue 3, 2018.

Technical surveys of single topics:

[S26] "Three XOR-Lemmas – An Exposition", *ECCC*, TR95-056, 1995.

[S27] "A Sample of Samplers – A Computational Perspective on Sampling", *ECCC*, TR97-020, May 1997.

[S28] "Notes on Levin's Theory of Average-Case Complexity", *ECCC*, TR97-058, 1997.

[S29] "On Security Preserving Reductions – Revised Terminology", *Cryptology ePrint Archive*, Report 2000/001, 2000.

[S30] "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.

[S31] Oded Goldreich, Dana Ron: Estimating Simple Graph Parameters in Sublinear Time. *Encyclopedia of Algorithms*, pages 650–653, 2006.

[S32] Oded Goldreich, Dana Ron: Testing Bipartiteness in the Dense-Graph Model. *Encyclopedia of Algorithms*, pages 2212–2216, 2006.

[S33] Oded Goldreich, Dana Ron: Testing Bipartiteness of Graphs in Sublinear Time. *Encyclopedia of Algorithms*, pages 2216–2219, 2006.

[S34] "On the doubly-efficient interactive proof systems of GKR", *ECCC*, TR17-101, June 2017.

[S35] "Overview of the doubly-efficient interactive proof systems of RRR", *ECCC*, TR17-102, June 2017.

3 Graduate Student Supervision

3.1 Graduate students who completed D.Sc./Ph.D.

D1 Hugo Krawczyk. *Pseudorandomness and Computational Difficulty*, Technion, Feb. 1990.

The thesis contains an improved algorithm for inferring general congruential generators; a novel construction of pseudorandom generators; investigations concerning the existence of sparse pseudorandom distributions; and results on the parallel and sequential composition of zero-knowledge protocols.

Hugo is a research scientist at IBM Research Division, Hawthorne, NJ, USA.

D2 Amir Herzberg. *Communication Networks in the Presence of Faults*, Technion, March 1991. Co-supervised by A. Segall.

The thesis contains works on the emulation of synchronous networks in the presence of faults; detecting errors in end-to-end communication; and introducing a quantitative approach to dynamic networks.

Amir is a faculty member of the Computer Science Department of Bar-Ilan University, Israel.

D3 Ran Canetti. *Studies in Secure Multi-Party Computation with Applications*, Weizmann Institute of Science, June 1995.

The thesis includes comprehensive studies of Asynchronous Secure Computation and Dynamic Security; a Byzantine Agreement protocol with optimal resiliency; and practical schemes for Proactive Security.

Ran is a faculty member of the Computer Science Department of Tel-Aviv University (Israel) and Boston University (US).

D4 Erez Petrank. *Knowledge Complexity versus Computational Complexity and the Hardness of Approximations*, Technion, May 1995.

The thesis includes a upper bound on the computational complexity of languages with logarithmic knowledge complexity; and a study of the Gap Location in Non-Approximability results.

Erez is a faculty member in the Computer Science Department at the Technion, Israel.

D5 Yehuda Lindell. *On the Composition of Secure Multi-Party Protocols*, Weizmann Institute of Science, July 2002. Co-supervised by M. Naor.

The thesis includes a comprehensive study of the preservation of the security of two-party and multi-party protocols under concurrent composition with and without fair termination requirements.

Yehuda is a faculty member in the Computer Science Department at Bar-Ilan University, Israel.

D6 Alon Rosen. *The Round-Complexity of Black-Box Concurrent Zero-Knowledge*, Weizmann Institute of Science, June 2003. Co-supervised by M. Naor.

The thesis provides matching lower and upper bounds on the round-complexity of concurrent zero-knowledge with respect to black-box simulations.

Alon is a faculty member in the Computer Science Department at the Herzliya Interdisciplinary Center, Israel.

D7 Boaz Barak. *Non-Black-Box Techniques in Cryptography*, Weizmann Institute of Science, January 2004.

The thesis demonstrates the power of non-black-box techniques. In particular, it contains zero-knowledge protocols that are proven zero-knowledge via non-black-box simulators, and have several features known to be unachievable via black-box simulators.

Boaz is a faculty member at Harvard University.

D8 Noam Livne. *From Computational Complexity to Cryptography and to Game Theory*, Weizmann Institute of Science, August 2010. Co-supervised by A. Rosen.

The thesis contains a method of coupling NP-complete problems with simple distributions (i.e., P-computable distributions) such that the resulting distributional problem is DistNP-complete.

Noam works in the industry.

D9 Or Meir. *Combinatorial Constructions of Probabilistic Proof Systems*, Weizmann Institute of Science, June 2011.

The thesis provides alternative proofs for several key results regarding probabilistic proof systems, while significantly reducing the reliance of abscure algebraic techniques.

Or is a faculty member at Haifa University.

D10 Ron Rothblum. *Verifiable Outsourcing of Computation*, Weizmann Institute of Science, March 2015.

The thesis studies two models of interactive proof systems in which the prover runs in polynomial-time and the verifier runs in nearly-linear time or sublinear-time, respectively.

Ron is a post-doc at MIT.

D11 Tom Gur. *On Locally Verifiable Proofs of Proximity*, Weizmann Institute of Science, February 2017.

The thesis studies several models of "locally verifiable proofs of proximity" including a new non-interactive model (coined MAP for MA proofs of Proximity).

Tom is a post-doc at UC-Berkeley.

3.2 Graduate students working towards Ph.D.

D12 Roei Tell. Interested in derandomization.

3.3 Graduate students who completed M.Sc.

M1 Ronen Vainish. *Improvements in a General Method for Constructing Cryptographic Protocols*, Technion, May 1988. (The thesis improves the efficiency of the automatic generator of fault-tolerant protocols presented by Goldreich, Micali and Wigderson.)

M2 Eyal Kushilevitz. *Perfect Zero-Knowledge Proofs*, Technion, March 1989. (The thesis presents a perfect zero-knowledge proof for a problem which is computationally equivalent to computing Discrete Logarithm.) [Eyal is a Professor of Computer Science at the Technion, Israel.]

M3 Tziporet Koren. *On the Construction of Pseudorandom Block Ciphers*, Technion, May 1989. (The thesis presents a proof for a theorem concerning pseudorandom permutation generators, stated but not proven by Luby and Rackoff.)

M4 Guy Even. *Construction of Small Probability Spaces for Deterministic Simulation*, Technion, Aug. 1991. (The thesis generalizes the definition and a construction of (k, ϵ)-distributions from the binary case to the p-ary case, where p is a prime power.) [Guy is a faculty member of the EE Department at Tel-Aviv University, Israel.]

M5 Erez Petrank. *Quantifying Knowledge Complexity*, Technion, Dec. 1991. (The thesis presents and investigates various definitions of knowledge complexity.) See [D4].

M6 Ran Canetti. *Quantitative Tradeoffs between Randomness and Communication Complexity*, Technion, Jan. 1992. (The thesis presents trade-off between randomness and communication in the context of communication complexity.) See [D3].

M7 Dror Sneh. *The Complexity of Global Computation in the Presence of Link Failures*, Technion, June 1992. (The thesis presents lower bounds on the message complexity of distributed computation in the presence of unidirectional link failures.)

M8 Ariel Kahan. *Constant-Round Zero-Knowledge Proofs*, Technion, Oct. 1992. (The thesis presents constant-round zero-knowledge proof systems for any language in NP, using clawfree permutation pairs.)

M9 Vered Rosen. *On the Security of Modular Exponentiation*, Weizmann Institute of Science, May 2000. (The thesis presents a study of the indistinguishability of modular exponentiation with random half-sized exponents versus random full-sized exponents.)

M10 Yoad Lustig. *Security Criteria for Public-Key Encryption*, Weizmann Institute of Science, October 2001. (The thesis consists of a study of semantic-security type definitions for chosen-ciphertext attacks as well as of definitions that refer to the security of multiple ciphertext in an adaptive setting.)

M11 Iftach Haitner. *Implementing Oblivious Transfer using Collection of Dense Trapdoor Permutations*, Weizmann Institute of Science, January 2004. (The thesis presents such a protocol using any collection of dense trapdoor permutations rather than a collection of enhanced trapdoor permutations.) [Iftach is a faculty member of the Computer Science Department at Tel-Aviv University, Israel.]

M12 Or Sheffet. *Reducing the Randomness Complexity of Property Testing, with an Emphasis on Testing Bipartiteness*, Weizmann Institute of Science, December 2006. (The thesis studies the randomness-complexity of property testing presenting both general existential bounds and specific efficient algorithms for the case of Bipartiteness.)

M13 Gilad Tsur. *Polylogarithmic Time and Query Complexity*, Weizmann Institute of Science, January 2007. (The thesis re-discovers and studies various classes of polylogarithmic time complexity.)

M14 Kfir Barhum. *Approximating Averages of Geometrical and Combinatorial Quantities*, Weizmann Institute of Science, February 2007. (The thesis presents fast algorithms for approximating the average distance between pairs of points in a Euclidean space and the average degree in a uniform hypergraph.)

M15 Or Meir. *Combinatorial Construction of Locally Testable Codes*, Weizmann Institute of Science, October 2007. (The thesis presents a new construction of LTCs that is purely combinatorial, does not rely on PCP machinery, and matches the parameters of the previously known construction.) See [D9].

M16 Yoav Tzur. *Notions of Weak Pseudorandomness and $GF(2^n)$-Polynomials*, Weizmann Institute of Science, October 2009. (The thesis studies the power and limitations of constructions of pseudorandom generators based on polynomial maps over the field $GF(2^n)$.)

M17 Lidor Avigad. *On the lowest level of query complexity in testing graph properties*, Weizmann Institute of Science, December 2009. (The thesis presents an optimal non-adaptive tester for the property of being a blow-up of a fixed graph.)

M18 Ron Rothblum. *On Homomorphic Encryption and Enhanced Trapdoor Permutations*, Weizmann Institute of Science, September 2010. (The thesis presents two independent studies of two remotely elated advanced cryptographic primitives.) See [D10].

M19 Aviv Reznik. *Finding k-paths in cycle-free graph*, Weizmann Institute of Science, December 2011. (The thesis presents an efficient algorithm for the cycle-free case.)

M20 Roei Tell. *Dual Problems in Property Testing*, Weizmann Institute of Science, August 2015. (The thesis initiates a study of dual testing problems, where a dual property consists of all objects that are far from the primary property.) See [D12].

M21 Maya Leshkowitz. *On Randomness Complexity and Round Complexity in Interactive Proofs*, Weizmann Institute of Science, March 2017. (The thesis shows that any set having an interactive proof system of randomness complexity r has an $o(r(n))$-round interactive proof system.)

3.4 Mentoring

(1) Yair Oren. Technion, 1986–88. Research regarding definitions and properties of zero-knowledge proof systems.

(2) Yishay Mansour. Technion, 1986/87. Research regarding completeness and soundness errors in interactive proof systems. [Yishay is a Professor of Computer Science at Tel-Aviv Universitry, Israel.]

(3) Shai Halevi. MIT, 1996/97. Research towards lattice-based cryptography. [Shai is a research scientist at IBM Research Division, Hawthorne, NJ, USA.]

(4) Salil Vadhan. MIT, 1997–99. Research regarding Statistical Zero-Knowledge, Pseudorandomness, and Randomness Extractors. [Salil is a Professor of Computer Science at Harvard University.]

(5) Amit Sahai. MIT, 1997/98. Research regarding Statistical Zero-Knowledge. [Amit is an Associate Professor at UCLA.]

(6) Igor Shinkar. Weizmann, 2010-13. Research regarding proximity oblivious testers.

(7) Avishay Tal. Weizmann, 2014/15. Research regarding the rigidity of Toeplitz matrices.

4 Postdoctoral fellows hosted

P1 Leonard (Yehuda) Schulman. Weizmann Institute of Science, 1994/5. Leonard is a Professor of Computer Science at the California Institute of Technology.

P2 Ronen Shaltiel. Weizmann Institute of Science, 2001–04. Ronen is a faculty member of the Department of Computer Science of Haifa University.

P3 Sofya Raskhodnikova. Weizmann Institute of Science, 2004–06. Sofya is a faculty member of the Computer Science Department of Boston University.

P4 Benny Applebaum. Weizmann Institute of Science, 2009/10. Benny is a faculty member of the EE Department at Tel-Aviv University, Israel.

P5 Tali Kaufman. Weizmann Institute of Science, 2009/10. Tali is a faculty member of the Department of Computer Science of Bar-Ilan University.

P6 Reut Levi. Weizmann Institute of Science, 2017/18.

5 Teaching Experience

5.1 Undergraduate Courses

(All in the Computer Science Dept., Technion, Israel):

- *Introduction to Programming* (sessions): 1981.
- *Discrete Mathematics*: 1983.
- *Graph Algorithms*: 1989.
- *Automata and Formal Languages*: 1986.
- *Theory of Computation*: 1987, 1988, 1989, 1990, 1991, 1992, 1993.

5.2 Graduate Courses

(All courses till 1993 – at the Technion, rest at the Weizmann):

- *Introduction to Property Testing*: Fall 2015.
- **Complexity Theory**
  - A yearly supervised-reading introductory course: 2012-13, 2014-15, 2016-17, and 2017-18.
  - A yearly introductory course: 1999-2000, 2005-06, 2007-08, and 2009-10.
  - A single-semester introductory course: 1991 and 2002.
  - Advanced topics: 1994.
- **Cryptography**
  - *Foundations of Cryptography* – supervised reading format: 2010-11 and 2013-14.
  - *Foundations of Cryptography* – two-semester format: 2004-05 and 2008-09.
  - *Foundations of Cryptography* – single-semester format: 1988, 1989, 1992, 2000, and 2002.
  - *Introduction to Cryptography*: 1994.
  - *Advanced Topics in Cryptography*: 1990 and 2001.
- *Probabilistic Methods in Complexity Theory*: 1991, 1993, and 2001.
- *Advanced Topics in Theoretical Computer Science*: 1986, 1988, and 1993.
- *Algebric Complexity of Computation* (sessions): 1983.

5.3 Short Courses and Lecture Series

- *Pseudorandomness*, lecture series at the IAS/Park City Mathematics Institute summer school, 2000.
- *Zero-knowledge*, toturial at the 43rd FOCS, 2002.

6 Positions

(The items in this section as well as in subsequent ones are listed in reversed chronological order.)

Sept. 2011 – Aug. 2012: Visiting scholar, Institute for Advanced Study, Princeton, NJ.

Sept. 2003 – June 2004: Fellow of the Radcliffe Institute for Advanced Study, Harvard University.

Since November 1998: The Meyer W. Weisgal Professorial Chair, Weizmann Institute of Science, Israel.

July 1995 – June 1998: Visiting Scientist, Laboratory for Computer Science, M.I.T, USA.

Since October 1995: Full Professor, Computer Science and Applied Mathematics Department, Weizmann Institute of Science, Israel.

March 1994 – Sept. 1995: Associate Professor (with tenure), Computer Science and Applied Mathematics Department, Weizmann Institute of Science, Israel.

July 1988 – Feb. 1994: Associate Professor (with tenure), Computer Science Department, Technion, Israel.

Jan. 1986 – June 1988: Senior Lecturer (Assistant Professor), Computer Science Department, Technion, Israel.

Feb. 1985 – Sept. 1986: Post-Doctoral Associate, Laboratory for Computer Science, M.I.T, USA.

July 1983 – Sept. 1984: Post-Doctoral Fellow, Laboratory for Computer Science, M.I.T, USA.

Oct. 1983 – Dec. 1985: Lecturer, Computer Science Department, Technion, Israel.

Oct. 1980 – Sept. 1983: Teaching Assistant, Computer Science Department, Technion, Israel.

7 Fellowships and Honors

- The *2017 Donald E. Knuth prize* for outstanding contributions to the foundations of computer science.
- Dedicated workshop on *Randommess, Complexity and Cryptography: The First Sixty Years of Oded Goldreich*, Weizmann Institute of Science, 19–20 April 2019.

  Dedicated volume holding *Tutorials on the Foundations of Cryptography* (Yehuda Lindell, editor), Information Security and Cryptography series, Springer, 2017.
- *Fellow of the International Association for Cryptologic Research*, 2009.
- Member of the *TCS Chair Professor Team*, Tsinghua University, 2007–2010.
- *RSA Conference 2006 Award for Excellence in the Field of Mathematics.*
- *Fellow of the Radcliffe Institute for Advanced Study*, Harvard University, 2003-04.
- *Corresponding Fellow of the Bavarian Academy of Sciences and Humanities*, since 2003.
- *Visiting Miller Research Professor*, Miller Institute for Basic Research in Science of the University of California at Berkeley, USA, 1996.
- *IBM Post-Doctoral Fellowship*, 1986.
- *Weizmann Post-Doctoral Fellowship*, 1983-84 and 1985.
- *Gutwirth Scholarship Award for Excellent Doctoral Student*, 1982, Technion, Haifa, Israel.
- *Gutwirth Scholarship Award for Excellent Master Student*, 1981, Technion, Haifa, Israel.

- *President's Undergraduate List of Excellence*, 1978-79, Technion, Haifa, Israel.
- *Chairman's Undergraduate List of Excellence*, 1977-78 and 1979-80, Computer Science Dept., Technion, Haifa, Israel.

8 Short Visits

October 2008: iTCS, Tsinghua University, Beijing, China.

April 2006: FIT, Tsinghua University, Beijing, China.

September 2002: Institute of Advanced Studies, Princeton, NJ, USA.

August 2000: Institute of Advanced Studies, Princeton, NJ, USA.

October 1996: Mathematical Sciences Department of IBM Thomas J. Watson Research Center, Yorktown Heights, NJ, USA.

August – September 1996: Computer Science Department of the University of California at Berkeley, USA.

September 1994: Basic Research in Computer Science (BRICS), Center of Danish National Research Foundation, Aarhus, Denmark.

July 1994: Network Architecture and Algorithms Group, Department of Communication Systems, Computer Science, IBM Research Division, Hawthorne, NJ, USA.

August 1993: International Computer Science Institute (ICSI), Berkeley, USA.

July 1993: Network Architecture and Algorithms Group, Department of Communication Systems, Computer Science, IBM Research Division, Hawthorne, NJ, USA.

August – September 1991: International Computer Science Institute (ICSI), Berkeley, USA.

August 1989: International Computer Science Institute (ICSI), Berkeley, USA.

July 1988: International Computer Science Institute (ICSI), Berkeley, USA.

July – August 1987: Laboratory for Computer Science, MIT, USA.

July 1982: Electronic Research Lab., UC-Berkeley, USA.

9 Special Invitations

9.1 Invited Speaker at Conferences

- Knuth Prize Lecture at the *49th Annual ACM Symposium on the Theory of Computing* (*49th STOC*), June 2017, Montreal, Canada.
- Invited speaker at the *14th Intl. Workshop on Randomization and Computation - RANDOM*, September 2010, Barcelona, Spain. Talk's title "Some Thoughts regarding Unconditional Derandomization".

- Invited speaker at the mini-symposium on Mathematical Cryptology in the *5th European Congress of Mathematics*, July 2008, Amsterdam, Netherlands. Talk's title "The Bright Side of Hardness".

- Invited speaker at the *27th International Colloquium on Automata Languages and Programming* (*ICALP'00*), July 2000, Genève, Swiss. Talk's title "Pseudorandomness".

- Invited speaker at *Crypto97*, August 1997, Santa Barbara, USA. Talk's title "The Foundations of Modern Cryptography".

- Invited speaker at the *14th Symposium on Theoretical Aspects of Computer Science* (*STACS97*), February/March 1997, Lübeck, Germany. Talk's title "Probabilistic Proof Systems".

- Invited speaker at the *International Congress of Mathematicians* (*ICM94*), August 1994, Zürich, Switzerland. Talk's title "Probabilistic Proof Systems".

- Invited speaker at the *Israel Mathematical Union annual meeting*, April 1994, Beer-Sheva, Israel. Talk's title "Probabilistic Proof Systems".

- Invited speaker at the *4th SIAM Conference on Discrete Mathematics*, June 1988, San Francisco, USA. Talk's title "Zero-Knowledge Proofs: Proofs that Yield Nothing But their Validity".

- Invited speaker at the *17th European Meeting of Statisticians*, August 1987, Thessaloniki, Greece. Talk's title "Proofs, Knowledge and Coin Tosses".

9.2 Participation in Workshops (by invitation)

- *Workshop on Local Algorithms*, October 2016, MSR and MIT, USA.

- *Workshop on Sublinear Algorithms*, January 2016, JHU, USA. Talk given "Testing Dynamic Environments".

- *Workshop on Complexity Theory*, November 2015, Oberwolfach, Germany. (Co-organizer)

- *Seminar on Computational Complexity of Discrete Problems*, March 2014, Dagstuhl, Germany. Talk given "Boolean Circuits of Depth Three and Arithmetic Circuits with Arbitrary Gates".

- *Workshop on Propoerty Testing*, June 2013, Haifa, Israel. Talks given "On Multiple Input Problems in Property Testing" and "On the Communication Complexity Methodology for Proving Lower Bounds on the Query Complexity of Property Testing".

- *Workshop on Complexity Theory*, November 2012, Oberwolfach, Germany. (Co-organizer)

- *Workshop on Sublinear Algorithms*, May 2011, Bertinoro, Italy. Talk given "Finding Cycles and Trees in Sublinear Time".

- *Workshop on Complexity Theory*, November 2009, Oberwolfach, Germany. (Co-organizer)

- *Workshop on Sublinear Algorithms*, August 2008, Dagstuhl, Germany.

- *Workshop on Cryptography*, September 2007, Dagstuhl, Germany.
- *Workshop on Complexity Theory*, June 2007, Oberwolfach, Germany. (Co-organizer)
- *Workshop on Randomness and Complexity*, July 2006, Bristol, England. Talk given "Pseudorandomness (an overview)".
- *Workshop on Sublinear Algorithms*, July 2005, Dagstuhl, Germany. Talk given "Contemplations on testing graph properties".
- *Workshop on Complexity Theory*, June 2005, Oberwolfach, Germany. (Co-organizer)
- *Workshop on Complexity Theory*, May 2003, Oberwolfach, Germany. (Co-organizer)
- *Workshop on Complexity Theory*, November 2000, Oberwolfach, Germany. (Co-organizer)
- *DIMACS Workshop on Sublinear Algorithms*, September 2000, Princeton, USA. Talk given "An Introduction to Property Testing".
- *Workshop on Complexity Theory*, November 1998, Oberwolfach, Germany. (Co-organizer)
- *Fields Institute Workshop on Interactive Proofs, PCP's and Fundamentals of Cryptography*, May 1998, Toronto, Canada. Talk given "Combinatorial Property Testing (a survey)".
- *DIMACS Workshop on Randomization Methods in Algorithm Design*, December 1997, Princeton, USA. Talk given "Combinatorial Property Testing (a survey)".
- *Workshop on Cryptography*, September 1997, Dagstuhl, Germany. Work presented "On the Limits of Non-Approximability of Lattice Problems".
- *Workshop on Complexity Theory*, November 1996, Oberwolfach, Germany. (Co-organizer)
- *Workshop on Randomized Algorithms and Computation*, December 1995, Berkeley, USA. Work presented "Non-Approximability Results for MAX SNP – Towards Tight Results".
- *Workshop on Cryptography*, September 1995, Luminy, France. Work presented "Information Theory versus Complexity Theory: another Test Case".
- *Weizmann Workshop on Randomness and Computation*, January 1995, Rehovot, Israel. (Co-organizer)
- *Workshop on Complexity Theory*, November 1994, Oberwolfach, Germany. Work presented "Knowledge Complexity".
- *Mini-workshop on Proof Verification and Approximation Algorithms*, March 1994, Oberwolfach, Germany.
- *Weizmann Workshop on Proabilistic Proof Systems and Cryptography, Program Checking and Approximation Problems*, January 1994, Rehovot, Israel. Work presented "Tiny Families of Functions with Random Properties".

- *Workshop on Cryptography*, September 1993, Dagstuhl, Germany. Work presented "Using Error-Correcting Codes to Enhance the Security of Signature Schemes or Security in Theory and Practice".

- *Workshop on Complexity Theory*, November 1992, Oberwolfach, Germany. Work presented "Towards a Computational Theory of Statistical Tests".

- *Workshop on Cryptography*, September 1989, Oberwolfach, W. Germany. Works presented "A Note on Computational Indistinguishability" and "A Uniform Complexity Treatment of Encryption and Zero-Knowledge".

- *Workshop on Mathematical Methods in VLSI and Distributed Computing*, November 1987, Oberwolfach, W. Germany. Work presented "How to Solve any Protocol Problem".

- *Workshop on Algorithms, Randomness and Complexity*, March 1986, Luminy, France. Work presented "Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity".

- *AMS Conference on Computational Number Theory*, August 1985, Arceta, USA.

- *Workshop on Cryptography*, June 1985, MIT – Endicott House, Massachusetts, USA. Work presented "Unbiased Bits from Weak Sources of Randomness".

9.3 Speaker in Special Colloquiums

- Invited speaker at IAS's *Celebration of Avi Wigderson's 60th birthday*, October 2016, Institute for Advanced Study, Princeton, USA. Talk's title "Canonical depth-three Boolean circuits for multi-linear functions, Multi-linear circuits with general gates, and matrix rigidity".

- Invited speaker at the *China Theory Week*, July 2013, Aarhus, Denmark. Talk's title "Property Testing: Sublinear-Time Approximate Decision".

- Invited speaker at the BIT's *conference in honour of Joachim von zur Gathen's 60th birthday*, May 2010, Bonn, Germany. Talk's title "General Cryptographic Protocols: A Brief Survey".

- Invited speaker at the Technion's *Shimon Even Memorial Lecture*, May 2008, Haifa, Israel. Talk's title "Probabilistic Proof Systems".

- Invited speaker at the *NYC Theory Day*, November 2003, New York, USA. Talk's title "On the Implementation of Huge Random Objects".

- Invited speaker at the *One-Day Colloquium in Honor of Shimon Even's 60th Birthday*, June 1995, Haifa, Israel. Talk's title "Free bits in PCPs and non-approximability – Towards tight results".

- Invited speaker at *Israeli Theory Seminar in Computer Science*, May 1991, Tel-Aviv, Israel. Talk's title "Fault-tolerant Computation in the Full Information Model".

- Invited speaker at *Israeli Theory Seminar in Computer Science*, January 1989, Tel-Aviv, Israel. Talk's title "A Hard-Core Predicate for any One-Way Function".
- Invited speaker at *Israeli Theory Seminar in Computer Science*, November 1986, Tel-Aviv, Israel. Talk's title "Proofs which Yield Nothing But their Validity or All NP Languages Have Zero-Knowledge Proofs".
- Invited speaker at the *Columbia 9th Theory Day*, September 1986, New York, USA. Talk's title "Proofs which Yield Nothing But their Validity or All NP Languages Have Zero-Knowledge Proofs".

10 Service on Departmental and Institutional Committees

All at the Weizmann Institute of Science.

1999–2001 and 2007–10: Member of the Institute's Hiring Committee (V9).

2001–03 and 2013–15: Head of the Department's Hiring Committee.

1999–2003 and 2009–10: Member of the Department's Hiring Committee.

2008–11: Representative of the Institute's Scientific Council on the *Inter-Senate Committee* (ISC) *of the Universities for Protection of Academic Independence*.

2008–10: Member of the Institute's Library Committee.

2004–07: Member of the Institute's Services Committee.

11 Public Professional Activities

11.1 Organization of Conferences and Workshops

Organization of Workshops:

- Organizer of the *Visions of Cryptography workshop*, December 2013, Rehovot, Israel.
- Co-organizer of the *Complexity Theory Meeting*, November 1996, November 1998, November 2000, April 2003, June 2005, June 2007, November 2009, November 2012, November 2015, and November 2018, Oberwolfach, Germany.
- Organizer of the *ITCS mini-Workshop on Property Testing*, January 2010, Beijing, China.
- Co-organizer of the *Weizmann Workshop on Randomness and Computation*, January 1995, Rehovot, Israel.

Service on Steering Committees of Conferences:

- Member of the Steering Committee of the *Innovations in (Theoretical) Computer Science* (*I(T)CS*), since being founded (in 2009) till 2016, and again since 2017.
- Member of the Steering Committee of the *Theory of Cryptography Conference* (*TCC*), since being founded (in 2003) till 2013.

  Chair 2005–2013.
- Member of the Steering Committee of the *International Workshop on Randomization and Computation* (*RANDOM*), since the late 1990's.

Service on Program Committees of Conferences:

- Member of the Program Committee for *STOC90*, *FOCS94*, *FOCS99* and *FOCS04*.
- Member of the Program Committee for *ITCS'18*.
- Member of the Program Committee for *Crypto85*, *Crypto88* and *Crypto92*.
- Member of the Program Committee for *Complexity03* and *Complexity09*.
- Member of the Program Committee for *PODC97*.
- Chairman of the Program Committee for the *2nd Israel Symp. on the Theory of Computing and Systems* (*ISTCS*), 1993.

11.2 Editorial and Refereeing Work

Editor of books or proceedings:

- Editor of the book *Property Testing*, Springer's LNCS, Vol 6390 (series "LNCS State-of-the-Art Surveys"), 2010.
- Co-editor of the book *Theoretical Computer Science: Essays in Memory of Shimon Even*, Festschrift series of Springer's LNCS, Vol 3895, March 2006.
- Editor of the proceedings of the *2nd Israel Symp. on the Theory of Computing and Systems* (*ISTCS*), IEEE Computer Society Press, 1993.

  Published a report on the conference in *SIGACT News*, Vol. 24, Nr. 3, October 1993.

Editor of journals and electronic depositories:

- Since being founded (in 2004): Member of the editorial board of Now's *Foundations and Trends in Theoretical Computer Science*.
- Since May 2003: Associate Editor of *Computational Complexity*.

  Editor of special issues on *Worst-Case Versus Average-Case Complexity* (together with Salil Vadhan, Vol. 16, Nr. 4, 2007), *Random'06* (Vol. 17, Nr. 1, 2008), *Random'09* (together with Salil Vadhan, Vol. 21, Nr. 1, 2012), and *10th TCC* (Vol. 25, Nr. 3, 2016).

- 1999-2016: On the advisory board of the Springer book series *Information Security & Cryptography*.
- 1996-2010: Member of the editorial board of *SIAM Journal on Computing*.

  Co-editor (together with Madhu Sudan) of special issue on *Randomness and Complexity* (Vol. 36-4, 2006).
- Since being founded (in 1994): Member of the editorial board of the *Electronic Colloquium on Computational Complexity* (*ECCC*), `http://www.eccc.uni-trier.de/eccc/`.

  Editor-in-Chief since 2017.
- 1992-2011: Member of the editorial board of *Journal of Cryptology*.

  Editor of special issues on *General Secure Multi-Party Computation* (Winter 2000) and *Encryption in the Bounded Storage Model* (Winter 2004).

Reviews and Refereeing:

- Wrote a Featured Review for *Mathematical Reviews*, [99d:68077ab], April 1999.
- Refereed numerous papers for many scientific journals including *JACM, SIAM Journal on Computing, Algorithmica, Combinatorica, JCSS, Journal of Algorithms, IEEE Transactions on Information Theory, Information and Computation, SIAM Journal on Discrete Mathematics, Computational Complexity, Random Strutures and Algorithms, Journal of Cryptography, Journal of Complexity, IPL, Mathematical Systems Theory, ACM Computing Surveys.*
- Refereed numerous papers for several conferences including many of the *STOC, FOCS, ICALP* conferences.

11.3 Opinion articles

The following non-technical publications address various aspects of the relevant research community and are viewed as service to that community.

- An essay titled "On Struggle and Competition in Scientific Fields" was published in *SIGACT News*, Vol. 43, Nr. 1, March 2012.
- An essay titled "On the status of intellectual values in TOC" (reporting a sociological study and presenting opinions), Nov 2011.

  See also the related essay titled "On Intellectual and Instrumental Values in Science", April 2012. Published in *SIGACT News*, Vol. 43, Nr. 2, June 2012.
- An essay titled "On our Duties as Scientists" was published in *SIGACT News*, Vol. 40, Nr. 3, September 2009.
- An educational article "On Teaching the Basics of Complexity Theory" in *Essays in Theoretical Computer Science in Memory of Shimon Even*, pages 348-374, 2006.

- A white-paper (co-authorded by Avi Wigderson) promoting a wide scientific perspective on the Theory of Computation.

  See extended abstract in *SIGACT News*, Vol. 28, 1997.

- An article addressing the sociological state of Theoretical Computer Science was published in *SIGACT News*, Vol. 23, Nr. 1, January 1992 (titled "Critique of some Trends in the TCS Community in Light of Two Controversies").

12 Essays related to the philosophy and sociology of science

The following (unpublished) essays address various aspects of the scientific project.[1]

- On Struggle and Competition in Scientific Fields, Jan. 2012.
- On Intellectual and Instrumental Values in Science, Apr. 2012.
- On Scientific Evaluation and its relation to Understanding, Imagination, and Taste, May 2012.
- Lessons from Kant: On Knowledge, Morality, and Beauty, June 2012.
- On the philosophical basis of computational theories, Feb. 2014.
- Content-Oblivious Quality Measures and the Control of Academia, July 2015.

See Section 11.3 for a list of opinion articles that are more related to the theory of computation.

13 Research Grants

13.1 Active

- *Israel Science Foundation (ISF)*, Jerusalem, Israel.

  Grant No. 671/13, 2013-17. Project: "Property Testing and Sublinear Algorithms: Graphs, Distributions, and Time-Evolving Environments" (with co-PI Dana Ron). First year budget 270,000NIS.

13.2 Past

- *Israel Science Foundation (ISF)*, Jerusalem, Israel.

  Grant No. 1041/08, 2008-11. Project: "Randomness and Computation". First year budget 184,000NIS.

- *Israel Science Foundation (ISF)*, Jerusalem, Israel.

  Grant No. 460/05, 2005-08. Project: "Short Locally Testable Codes and Proofs". First year budget 150,000NIS.

[1] They are available from the website `http://www.wisdom.weizmann.ac.il/~oded/essays.html`.

- *Israel Internet Association (ISOC-IL).*

  A single year granted awarded Dec 2004. Project: "Sublinear-Time Algorithms for Networks" (with co-PI Dana Ron). Total budget 30,000$.

- *United States - Israel Binational Science Foundation (BSF)*, Jerusalem, Israel.

  Grant No. 92-00226, 1993–95. Project: "Randomness and Computation". Total budget 78,500$.

- *United States - Israel Binational Science Foundation (BSF)*, Jerusalem, Israel.

  Grant No. 89-00312, 1990–92. Project: "Pseudorandomness and Zero-Knowledge". Total budget 75,000$.

- *Fund for Basic Research Administered by the Israeli Academy of Sciences and Humanities.*

  Grant no. 570/86 (cont. 608/88), 1987–89. Title "Zero-Knowledge and Interactive Proof Systems". Total budget 38,560$.

- *United States - Israel Binational Science Foundation (BSF)*, Jerusalem, Israel.

  Grant No. 86-00301, 1987–89. Project: "Fault-Tolerant Distributed Protocols, Randomness and Computational Number Theory". Total budget 37,000$.

14 Patents

- B. Chor, O. Goldreich and E. Kushilevitz, "Private Information Retrieval", U.S. Patent No. 5,855,018 (issued on Dec. 29th 1998).

- O. Goldreich and R. Ostrovsky, "Comprehensive Software Protection System", U.S. Patent No. 5,123,045 (issued Jun. 16th 1992).

- S. Even, O. Goldreich and S. Micali, "On-Line/Off-Line Digital Signing", U.S. Patent No. 5,016,274 (issued May 14th 1991).