Curriculum Vitae

Oded Goldreich

January 1, 2012

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 9932157.

Research Interests and Expertise:

- Main current focus: Randomness and Computation.

  In particular, Property Testing, Pseudorandomness, and Probabilistic Proof Systems.
- Expertise: Foundations of Cryptography.
- Additional interest: Complexity Theory.
- 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 **1**
- 1.1 Randomized Computations . . . 1
  - 1.1.1 Pseudorandomness . . . 1
  - 1.1.2 Probabilistic Proof Systems . . . 2
  - 1.1.3 New Topics in Randomized Computations . . . 3
  - 1.1.4 Other Topics in Randomized Computations . . . 4
- 1.2 Foundations of Cryptography . . . 10
  - 1.2.1 Zero-Knowledge and Protocol Design . . . 10
  - 1.2.2 Pseudorandomness . . . 11
  - 1.2.3 New Topics in Cryptography . . . 11
  - 1.2.4 Other Topics in Cryptography . . . 11
- 1.3 Other Areas of the Theory of Computation . . . 15

2 Expository Contributions **18**
- 2.1 Books and Lecture Notes . . . 18
- 2.2 Survey articles . . . 19

3 Graduate Student Supervision **21**
- 3.1 Graduate students completed D.Sc. . . . 21
- 3.2 Graduate students working towards D.Sc. . . . 23
- 3.3 Graduate students completed M.Sc. . . . 23
- 3.4 Mentoring . . . 24

4 Postdoctoral fellows hosted **25**

5 Teaching Experience **25**
- 5.1 Undergraduate Courses . . . 25
- 5.2 Graduate Courses . . . 25
- 5.3 Short Courses and Lecture Series . . . 26

6 Positions **26**

7 Fellowships and Honors **27**

8 Short Visits **27**

9 Special Invitations **28**
- 9.1 Invited Speaker at Conferences . . . 28
- 9.2 Participation in Workshops (by invitation) . . . 28
- 9.3 Speaker in Special Colloquiums . . . 30

10 Service on Departmental and Institutional Committees **31**

11 Public Professional Activities **31**
- 11.1 Organization of Conferences and Workshops . . . 31
- 11.2 Editorial and Refereeing Work . . . 32
- 11.3 Opinion articles . . . 33

12 Research Grants **33**
- 12.1 Active . . . 33
- 12.2 Past . . . 33

13 Patents **34**

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*, *small probability spaces*, and *weak random sources*), and to cryptography (e.g., *zero-knowledge* and *fault-tolerant protocols*). These areas are somewhat overlapping so the partition adopted below is somewhat arbitrary. 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 [127].
- Showing how to solve any multi-party protocol problem, using any trapdoor permutation [128].
- Presenting a generic hardcore predicate for any one-way function [47].
- Showing how to construct pseudorandom functions from any pseudorandom generators [35].

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

1.1 Randomized Computations

Randomness is a central aspect of the theory of computation. The effects of randomness on computation can be appreciated from a variety of points of view ranging from the abstract study of complexity classes to the concrete construction of efficient algorithms. In particular, the notions of pseudorandom generators, interactive proofs, probabilistically checkable proofs (PCP), property testing, weak random sources and constructions of small probability spaces have played an important role in the development of complexity theory and in the analysis of algorithms. I am proud of having contributed to the development and understanding of these notions.

1.1.1 Pseudorandomness

Loosely speaking, a pseudorandom generator is an efficient (i.e., polynomial-time) deterministic algorithm that stretches a uniformly chosen *seed* into a much longer sequence that, nevertheless, looks random to and efficient observer. Pseudorandom generators allow to shrink the amount of randomness, in any efficient application, by an constant power (i.e., instead of using n uniformly chosen bits, the application can be modified to use only n^ϵ uniformly chosen bits, where $\epsilon > 0$ is any constant). The construction of pseudorandom generators, under various intractability assumptions, has been a major enterprise in the last couple of decades.

A key tool in the construction of pseudorandom generators is the construction of hard-core predicates. A hard-core predicate of the function f is a polynomial-time computable predicate of x which is hard to approximate from $f(x)$. Together with Levin [47], I was able to prove that any one-way function of the form $f(x,r) = (f'(x), r)$ has a hard-core predicate (specifically, the inner-product mod 2 of x and r). This result plays an important role in the area of pseudorandomness. In particular, our result yields a very simple construction of a pseudorandom generator based on any one-way *permutation* and was used (by Hastad, Impagliazzo, Levin and Luby) to construct a pseudorandom generator based on any one-way *function*. Our result improves over a previous general result of Yao and over previous results concerning specific functions of Blum and Micali,

and Alexi, Chor, Schnorr and myself [2]. Put in more general terms, the result in [47] asserts that the complexity of any search problem is related to the complexity of answering "random (linear) queries" concerning the solution. Namely, for a search problem R, if it is infeasible, on input x, to find a solution s such that $(x,s)\in R$ then it is also infeasible to predict the inner-product (mod 2) of s and r, when given x and r, for a uniformly chosen r. This general form found many additional applications.

Another contribution to the construction of pseudorandom generators is presented in [45]. This work contains a construction of pseudorandom generators based on any "regular" function. (Loosely speaking, a function f is called regular if each of its images has the same number of preimages.) The construction used in [45] utilizes *hash functions* in order to preserve the difficulty of successive iterations of a (regular) one-way function. Traces of this paradigm can be seen in many subsequent works in the area.

The theory of pseudorandomness has been extended to functions by Goldwasser, Micali and myself [35]. In particular, it has been shown how to construct pseudorandom functions, using an arbitrary pseudorandom (bit) generator. This means that a black-box that has only k secret bits of storage can implement a function from k-bit strings to k-bit strings that cannot be distinguished from a random function by any poly(k)-time observer that can "query the function" on arguments of his choice.

Other works of mine in the area of pseudorandomness include [44, 26, 78, 39, 48, 53, 51, 66, 36, 32]. In particular, in [26] I've shown that two efficiently sampleable distributions that are statistically different can be computational indistinguishable only if one-way functions exist. In [39] an efficient amplification of one-way permutations is presented. Amplification of one-way function is an important tool, especially in the construction of pseudorandom generators. In [36] a general study of the implementation of huge random object has been initiated. In [32] the pseudorandomness-to-derandomization connection is reversed.

1.1.2 Probabilistic Proof Systems

Various types of *probabilistic* proof systems have played a central role in the development of computer science in the last couple of decades. I have contributed to the development of three such proof systems: *interactive proofs*, *zero-knowledge proofs*, and *probabilistic checkable proofs*.

Interactive Proofs. Interactive proof systems were presented by Goldwasser, Micali and Rackoff as a randomized and (more) interactive generalization of $\mathcal{NP}$. The generalization was aimed at providing a convenient framework for the presentation of zero-knowledge proofs. (In fact, in [129] it was proved that this generalization is indeed essential for the (non-trivial) existence of zero-knowledge proofs.) However, back in 1985, it was not clear whether interactive proofs are more powerful than $\mathcal{NP}$. First evidence to the power of interactive proof systems was given by Micali, Wigderson and myself, by showing that Graph Non-Isomorphism (which is not known to be in $\mathcal{NP}$) has an interactive proof system [127]. Still, the focus of that paper is on the zero-knowledge aspects of interactive proofs: see Section 1.2.

In [17], interactive proofs were used to present a dramatic refutation to the Random Oracle Hypothesis. In contrast to co$\mathcal{NP}\subseteq\mathcal{IP}$ (estblaished before by Lund, Fortnow, Karloff and Nisan), we showed that, *relative to a random oracle*, co$\mathcal{NP}$ is not contained in $\mathcal{IP}$.

More refined studies of the role of interaction, randomness and error probability in interactive proof systems are the subject of [25, 8, 40, 71]. In particular, in [25] it is shown that the error probability in the completeness condition of interactive proof systems is unessential. In [8] the

problem of efficient error-reduction in interactive proofs is addressed. This work also presents a randomness-efficient sampling algorithm that is of independent interest. The power (or rather limitations) of interactive proof systems with bounded communication is studied in [40, 71].

Zero-Knowledge and Knowledge Complexity. A fundamental complexity measure associated with interactive proof systems is their knowledge complexity. The special case of knowledge complexity zero (aka Zero-knowledge) has received a lot of attention and is discussed in the Section 1.2. The general notion (of knowledge complexity) was suggested by Goldwasser, Micali and Rackoff, yet without satisfactory definition (for the case where this complexity is greater than zero). In [55], two satisfactory definitions were presented and shown equivalent up to a constant. In [54], evidence was given to show that not all languages in $\mathcal{IP}$ have interactive proof systems of small (e.g., up to logarithmic) knowledge complexity.

Probabilistically Checkable Proofs. Probabilistic checkable proof (PCP) systems have been a focus of intensive research, mainly due to the FGLSS-methodology of proving hardness results for combinatorial approximation problems. In [9], we show that this methodology is "complete" in the following sense. We study the free-bit complexity, denoted f, of probabilistic verifiers for NP and show that an NP-hardness result for the approximation of MaxClique to within a factor of $N^{1/(g+1)}$ would imply $f \leq g$. In addition, we reduce this complexity to two (i.e., $f \leq 2$) which yields (via the FGLSS-method) that approximating the clique to within a factor of $N^{1/3}$ (in an N-vertex graph) is NP-hard. We also obtain improved non-approximability results for other Max-SNP problems such as Max-2SAT and Max-3SAT. Underlying all these complexity improvements was the suggestion to use a new code in the inner-most level of the proof system, and the development of corresponding codeword tests. This code, known as the LongCode, has been instrumental to further developments in the area, which include optimal NP-Hardness factors for MaxClique, Max3SAT, and some other problems (by Hastad).

Probabilistic checkable proofs of almost-linear length for SAT are presented in [67]: The length of the proof is approximately $n \cdot \exp(\sqrt{\log n})$ and verification in performed by a constant number (i.e., 19) of queries, as opposed to previous results that used proof length $n^{1+O(1/q)}$ for verification by q queries. The study of the trade-off between the length of PCPs and their query complexity is further pursued in [11]: In particular, we present PCPs of double-logarithmic query complexity while incurring only a quasi-polylogarithmic overhead (over the standard NP-proof) in the proof length. Our techniques include the introduction of a new variant of PCPs that we call "Robust PCPs of Proximity". These new PCPs facilitate proof composition, which is a central ingredient in construction of PCP systems.

1.1.3 New Topics in Randomized Computations

Property Testing. Together with Goldwasser and Ron, I have initiated a study of general property testing and its relation to learning theory and to approximation problems [37]. Property testing is a relaxation of a decision task, where one tries to distinguish between objects having the predetermined property and objects "being far" from having the property, and do so without inspecting the entire object. Our work [37] focuses on testing graph properties, and presents algorithms, running in time that does not depend on the size of the graph, that distinguish the case the graph has some predetermined property (e.g., being Bipartite) from the case it is far from the class of graphs having this property.

Follow-up works include [56, 57, 38, 23, 58, 69, 65, 61, 62, 5, 43]. In particular, while [37] refers to testing in a model that became known as the *dense graph model*, the bounded-degree graph model was introduced in [56] and its study was initiated in [56, 57]. The algorithmic aspects of the dense graph model were the focus of [69, 61]. The notion of a *proximity oblivious tester* was systematically studied in [62], whereas other graph algorithmic problems related to testing are studied in [60, 6, 22].

Locally testable codes. Locally testable codes are error-correcting codes that admit very efficient codeword tests. Specifically, using a constant number of (random) queries, non-codewords are rejected with probability proportional to their distance from the code. A systematic study of these codes was initiated in [67], which presents such (linear) codes in which k information bits are encoded by a codeword of length approximately $k \cdot \exp(\sqrt{\log k})$. Further improvements are presented in [11].

Locally decodable codes are different from locally testable codes, which are studied in [147]. The latter are closely related to private information retreival schemes, introduced in [97]. A relaxed form of locally decodable codes was presented in [11].

1.1.4 Other Topics in Randomized Computations

Construction of Small Sample Spaces. A careful investigation of *many* randomized algorithms reveals the fact that they perform as well when their random input only possesses *weak random properties* (rather than being uniformly distributed). Consequently, the construction of small sample spaces that exhibit some desired (weak) random properties is the key to transforming these algorithms into deterministic ones at a reasonable cost. An archetypical example is Luby's Maximal Independent Set algorithm. The construction of small sample spaces, inducing weak randomness properties, is addressed in [20, 18, 3, 24]. The first two works deal with *generating* and using constant amount of independence between the random variables, whereas the last two works deal with *approximating* larger amounts of independence. In particular, [3] contains three simple constructions of small sample spaces that are almost unbiased, and [24] contains general constructions for approximating any product-distribution.

Universal Hashing are used in many works in complexity theory. These works typically use two random properties of hash functions (i.e., "extraction" and "mixing"). In [72], we construct small families of functions having these random properties, demonstrating a trade-off between the quality of the functions and the size of the families from which they are drawn. For the "mixing" property and some parameters of the "extraction" problem, these constructions are still the best known.

Using Sources of Weak Randomness. The above mentioned works capitalize on the fact that *particular* randomized algorithms perform as well when their input is taken from a source of weak randomness. A complementary approach is to transform *any* randomized algorithm into a more robust algorithm so that the robust algorithm, when fed with a random input produced by a source of weak randomness, performs as well as the original algorithm when given a random input produced by a perfect source. This way of using sources of weak randomness in algorithms and other algorithmic settings is investigated in [18, 19]. In [19], Chor and myself introduce and investigate *probability bounded* sources of randomness that output a stream of *blocks* so that no string is "too likely" to appear in the next block. The notion of a probability-bounded source (a.k.a *min-entropy* source) turned out to be central to subsequent developments in this area, and the notion of a block-source played an important role too.

Probabilistic Communication Complexity. Another area in which randomness plays a central role is communication complexity. Here the setting consists of two parties each having an input and a predetermined two-argument function. The goal is to exchange as little bits of communication in order to obtain the value of the function. In [19], a tight relation between the problem of extracting unbiased bits from two weak sources and probabilistic communication complexity is established, leading in turn to tight bounds on the probabilistic communication complexity of most functions and of specific functions such as inner-product mod 2. Tradeoffs between randomness and communication were investigated in [16].

Publications in this area

[1] 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.

[2] W. Alexi, B. Chor, O. Goldreich, and C.P. Schnorr, "RSA/Rabin Functions: Certain Parts Are As Hard As the Whole", *SIAM Jour. on Computing*, Vol. 17, No. 2, April 1988, pp. 194–209. Extended abstract in *25th FOCS*, 1984.

[3] N. Alon, O. Goldreich, J. Hastad, and R. Peralta, "Simple Constructions of Almost k-wise Independent Random Variables, *Jour. of Random Structures and Algorithms*, Vol. 3, No. 3, pp. 189–304, 1992. Extended abstract in *31st FOCS*, 1990.

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

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

[6] K. Barhum, O. Goldreich and A. Shraibman, "On approximating the average distance between points", in the proceedings of *11th RANDOM*, Springer LNCS, Vol. 4627, pages 296–310, 2007.

[7] 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.

[8] M. Bellare, O. Goldreich, and S. Goldwasser, "Randomness in Interactive Proofs", *Computational Complexity*, Vol. 4, No. 4 (1993), pp. 319–354. Extended abstract in *31st FOCS*, 1990.

[9] M. Bellare, O. Goldreich and M. Sudan, "Free Bits and Non-Approximability", *SICOMP*, Vol. 27, No. 3, pp. 804–915, June 1998. Extended abstract in *36th FOCS*, 1995.

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

[11] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. "Robust PCPs of Proximity, Shorter PCPs and Applications to Coding", *SICOMP* (special issue on Randomness and Complexity), Volume 36, Issue 4, pages 889–974, 2006. Extended abstract in *36th STOC*, 2004.

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

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

[14] M. Blum and O. Goldreich, "Towards a Computational Theory of Statistical Tests", *33rd FOCS*, 1992.

[15] R. Canetti, G. Even and O. Goldreich, "Lower Bounds for Sampling Algorithms", *IPL 53* (1995), pp. 17–25.

[16] R. Canetti and O. Goldreich, "Bounds on Tradeoffs between Randomness and Communication Complexity", *Computational Complexity*, Vol. 3 (1993), pp. 141–167. Extended abstract in *31st FOCS*, 1990.

[17] 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.

[18] 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*, 1985, pp. 396–407.

[19] B. Chor and O. Goldreich, "Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity", *SIAM Jour. on Computing*, Vol. 17, No. 2, April 1988, pp. 230–261. Extended abstract in *26th FOCS*, 1985.

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

[21] B. Chor, O. Goldreich and S. Goldwasser, "The Bit Security of Modular Squaring given Partial Factorization of the Moduli", in *Advances in Cryptology – Crypto '85 (Proceedings)*, pp. 448–457, 1986.

[22] A. Czumaj, O. Goldreich, D. Ron, C. Seshadhri, A. Shapira, and C. Sohler, "Finding Cycles and Trees in Sublinear Time",

[23] 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.

[24] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Veličković, "Efficient Approximations of Product Distributions", *Random Structures and Algorithms*, Vol. 13, No. 1, pp. 1–16, Aug. 1998. Extended abstract in *24th STOC*, 1992.

[25] M. Furer, O. Goldreich, Y. Mansour, M. Sipser, and S. Zachos, "On Completeness and Soundness in Interactive Proof Systems", *Advances in Computing Research: a scientific annual*. Extended abstract in *28th FOCS*, 1987.

[26] O. Goldreich, "A Note on Computational Indistinguishability", *IPL 34* (1990), pp. 277–281.

[27] O. Goldreich, "Candidate One-Way Functions Based on Expander Graphs", *Cryptology ePrint Archive*, Report 2000/063, 2000. Also *ECCC*, TR00-090, 2000.

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

[29] O. Goldreich, "On the Average-Case Complexity of Property Testing", *ECCC*, TR07-057, 2007.

[30] O. Goldreich, "A Candidate Counterexample to the Easy Cylinders Conjecture", ECCC, Report TR09-028, Apr. 2009

[31] O. Goldreich. "On Testing Computability by Small Width OBDDs", Proceedings of *14th RANDOM*, Springer LNCS, Vol. 6302, pages 574–586, 2010.

[32] O. Goldreich. "In a World of P=BPP", ECCC TR10-135, 2010.

[33] O. Goldreich. "Two Comments on Targeted Canonical Derandomizers", ECCC TR11-047, 2011.

[34] O. Goldreich and S. Goldwasser, "On the Limits of Non-Approximability of Lattice Problems", *JCSS*, Vol. 60, pages 540–563, 2000. Extended abstract in *30th STOC*, 1998.

[35] 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. Extended abstract in *25th FOCS*, 1984.

[36] O. Goldreich, S. Goldwasser and A. Nussboim. "On the Implementation of Huge Random Objects", *SICOMP*, Vol. 39, No. 7, May 2010. Extended abstract in *44th FOCS*, 2003.

[37] O. Goldreich, S. Goldwasser and D. Ron, Property Testing and its connection to Learning and Approximation, *Journal of the ACM*, pages 653–750, July 1998. Extended abstract in *37th FOCS*, 1996.

[38] O. Goldreich, S. Goldwasser, E. Lehman, D. Ron and A. Samorodnitsky, Testing Monotinicity, *Combinatorica*, Vol. 20 (3), pages 301–337, 2000. Extended abstract in *39th FOCS*, 1998.

[39] O. Goldreich, R. Impagliazzo, L.A. Levin, R. Venkatesan, and D. Zuckerman, "Security Preserving Amplification of Hardness", extended abstract in *31st FOCS*, 1990.

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

[41] O. Goldreich and R. Izsak. "Monotone Circuits: One-Way Functions versus Pseudorandom Generators", ECCC TR11-121, 2011.

[42] O. Goldreich, B. Juba, and M. Sudan, "A Theory of Goal-Oriented Communication", ECCC, Report TR09-075, Sept. 2009

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

[44] O. Goldreich and H. Krawczyk, "On Sparse Pseudorandom Ensembles", *Random Structures and Algorithms*, Vol. 3, pp. 163–174, 1992.

[45] O. Goldreich, H. Krawczyk, and M. Luby, "On the Existence of Pseudorandom Generators". *SIAM J. on Computing*, Vol. 22-6 (1993), pp. 1163–1175. Extended abstract in *29th FOCS*, 1988.

[46] O. Goldreich, M. Krivelevich, I. Newman, and E. Rozenberg, "Hierarchy Theorems for Property Testing", In the proceedings of *13th RANDOM*, Springer LNCS, Vol. 5687, pages 504-519, 2009.

[47] O. Goldreich and L.A. Levin, "A Hard-Core Predicate for any One-Way Function". extended abstract in the proceedings of *21th STOC*, 1989.

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

[49] O. Goldreich and O. Meir, "The Tensor Product of Two Good Codes Is Not Necessarily Robustly Testable", *ECCC*, TR07-062, 2007.

[50] O. Goldreich and O. Meir. "Input-Oblivious Proof Systems and a Uniform Complexity Perspective on P/poly", *ECCC*, TR11-023, 2011.

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

[52] 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.

[53] O. Goldreich, N. Nisan and A. Wigderson, "On Yao's XOR-Lemma", *ECCC*, TR95-050, 1995.

[54] O. Goldreich, R. Ostrovsky and E. Petrank, "Knowledge Complexity and Computational Complexity", *SICOMP*, Volume 27, Number 4, pp. 1116–1141, August 1998. Extended abstract in the proceedings of *26th STOC*, 1994.

[55] O. Goldreich and E. Petrank, "Quantifying Knowledge Complexity", *Computational Complexity*, Vol. 8, pages 50–98, 1999. Extended abstract in *32nd FOCS*, 1991.

[56] O. Goldreich and D. Ron, Property Testing in Bounded Degree Graphs, *Algorithmica*, 32 (2), pages 302–343, 2002. Extended abstract in *29th STOC*, 1997.

[57] O. Goldreich and D. Ron, A Sublinear Bipartite Tester for Bounded Degree Graphs, *Combinatorica*, Vol. 19 (3), pages 335–373, 1999. Extended abstract in *30th STOC*, pp. 289–298, 1998.

[58] O. Goldreich and D. Ron, "On Testing Expansion in Bounded-Degree Graphs", *ECCC*, TR00-020, 2000.

[59] O. Goldreich and D. Ron, "On Estimating the Average Degree of a Graph", *ECCC*, TR04-013, 2004.

[60] O. Goldreich and D. Ron, "Approximating Average Parameters of Graphs", *Jour. of Random Structures and Algorithms*, Volume 32, Number 3, pages 473–493, 2008. Extended abstract in *10th RANDOM*, Springer LNCS, Vol. 4110, pages 363–374, 2006.

[61] O. Goldreich and D. Ron, "Algorithmic Aspects of Property Testing in the Dense Graphs Model", *SICOMP*, Vol. 40, No. 2, pages 376–445, 2011. Extended abstract in *13th RANDOM*, Springer LNCS, Vol. 5687, pages 520–533, 2009.

[62] O. Goldreich and D. Ron, "On Proximity Oblivious Testing", *SICOMP*, Vol. 40, No. 2, pages 534–566, 2011. Extended abstract in proceedings of the *41st STOC*, pages 141–150, 2009.

[63] 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.

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

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

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

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

[68] O. Goldreich, M. Sudan and L. Trevisan, "From logarithmic advice to single-bit advice", *ECCC*, TR04-093, 2004.

[69] O. Goldreich and L. Trevisan, "Three Theorems regarding Testing Graph Properties", *Journal of Random structures and Algorithms*, Vol. 23 (1), pages 23–57, August 2003. Extended abstract in *42th FOCS*, 2001.

[70] O. Goldreich, S. Vadhan and A. Wigderson, "Simplified Derandomization of BPP using a Hitting Set Generator" *ECCC*, TR00-004, 2000.

[71] O. Goldreich, S. Vadhan and A. Wigderson, "On interactive proofs with a laconic provers", *Computational Complexity*, Vol. 11, pages 1–53, 2002. Extended abstract in *28th ICALP*, 2001.

[72] O. Goldreich and A. Wigderson, "Tiny Families of Functions with Random Properties", *Journal of Random structures and Algorithms*, Volume 11, Number 4, December 1997, pages 315–343. Extended abstract in *26th STOC*, 1994.

[73] O. Goldreich and A. Wigderson, On the Circuit Complexity of Perfect Hashing, *ECCC*, TR96-041, 1996.

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

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

[76] O. Goldreich and A. Wigderson, "Derandomization that is rarely wrong from short advice that is typically good", Proceedings of *RANDOM*, pages 209–223, 2002.

[77] O. Goldreich and D. Zuckerman, "Another proof that BPP subseteq PH (and more)", *ECCC*, TR97-045, 1997.

Unpublished manuscripts in this area (cited in literature)

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

1.2 Foundations of Cryptography

I have participated in the revolutionary developments that have transformed the field of Cryptography from a semi-scientific discipline to a respectable field in theoretical computer science. Indeed, since the mid 1980's, Cryptography not only has its own merits but also sheds light on fundamental issues concerning computation such as randomization, knowledge and interaction.

1.2.1 Zero-Knowledge and Protocol Design

Zero-Knowledge Proofs. My most important contribution to the area is the work on zero-knowledge, coauthored by Micali and Wigderson [127]. In this work we demonstrate the generality and wide applicability of *zero-knowledge proofs*, a notion introduced by Goldwasser, Micali and Rackoff. These are probabilistic and interactive proofs that, for the members x of a language L, efficiently demonstrate membership in the language without conveying any additional knowledge. Until then, zero-knowledge proofs were known only for some number theoretic languages in $\mathcal{NP} \cap \text{co}\mathcal{NP}$. Assuming the existence of one-way functions, we showed that every language in NP has a zero-knowledge proof. Loosely speaking, it is possible to demonstrate that a CNF formula is satisfiable without revealing any other property of the formula. In particular, without yielding neither a satisfying assignment nor properties such as whether there is a satisfying assignment in which $x_1 = x_3$ etc. The dramatic effect of the above work on the design of cryptographic protocols is demonstrated in another paper of the same authors [128]. Indeed, zero-knowledge proofs have become a standard tool in the design of cryptographic schemes and protocols.

Other works of mine in the area of zero-knowledge proof systems include [129, 124, 123, 112, 122, 82, 98, 132, 134, 133, 121, 94, 80, 113, 79]. A common theme in many of these works is the attempt to uncover the principles underlying the phenomenon of zero-knowledge so that they can be better tuned towards applications. In particular, in [129, 112, 123], various formulations of zero-knowledge are suggested and investigated and certain properties of proof systems are demonstrated essential to the zero-knowledge property. In [98, 132], techniques for designing zero-knowledge proofs are developed; specifically, these works present compilers that given proof systems that are zero-knowledge w.r.t honest-verifier produce systems that are zero-knowledge against any verifier. In [121, 94, 80], the notion of *resettable zero-knowledge* was introduced and studied.

Cryptographic Protocol Design. The work on general multi-party computations coauthored by Micali, Wigderson and myself [128] is central to this area. Building on [127] and using additional ideas, we showed that any *protocol problem* can be solved. Specifically, for every m-ary (computable) function f, we construct a secure (fault-tolerant) m-party protocol for computing f on inputs scattered among the m parties. The protocol can tolerate adversarial behaviour of any minority, and no minority can learn from the execution more than it can learn from its own inputs and the value of the function. In other words, the protocol "emulates" a trusted party in a setting in which no party can be trusted (and furthermore any minority may be malicious). The construction of

the fault-tolerant protocol is explicit (in the sense that an efficient algorithm is presented that, on input a Turing machine description of a function, outputs the desired fault-tolerant protocol). This work [128] has also inspired the development and study of cryptographic protocols in the private channel model.

Other works of mine in the area of cryptographic protocols include [135, 89, 93]. In [135] it is shown that general multi-party computation reduces to a very simple two-party computation (of a two-bit function). In [89] the scope of multi-party computation is extended to the asynchronous setting, whereas [93] deals with adaptive/dynamic adversaries (in both the private channel and the computational models). Early works on testing and designing simple protocols appear in [101, 108, 105, 103, 109, 91, 106].

1.2.2 Pseudorandomness

Pseudorandom generators and functions, surveyed in Section 1.1, are very important to cryptography. In particular, pseudorandom functions yield private-key encryption and message-authentication schemes. Pseudorandom functions have become an important cryptographic tool used in a variety of applications. Early applications of pseudorandom functions were described in [120, 111, 110].

Results from cryptography (and in particular pseudorandom functions [35]) were used to derive many of the impossibility results in the area of machine learning.

1.2.3 New Topics in Cryptography

The notion of *incremental cryptography* was introduced and developed in [85, 86]. The aim of this approach is to design cryptographic algorithms (e.g., for signing) with the property that having applied the algorithm to a document, it is possible to quickly update the result of the algorithm for a modified document, rather than having to re-compute it from scratch. In particular, schemes that support powerful update operation and satisfy strong security requirements were developed yielding an application to the problem of virus protection (which was not possible before).

In [97], we consider the problem of *private information retreival*. In particular, we obtained several efficient schemes for obtaining a record from a database by querying servers maintaining duplicated copies of the database so that none of the individual servers can know which record has been required by the user.

Other work of an initiatory flavor include a critical review of the *Random Oracle Methodology* [95], a theoretical treatment of software protection [111], and a study of the (im)possibility of "code obfuscation" [81].

1.2.4 Other Topics in Cryptography

I have also worked on the "classical" problems of cryptography, namely encryption [112] and signatures [110, 104]. In particular, in [104] the notion of an On-line/Off-line Signature Scheme is presented and instantiated.

Publications in this area

[79] B. Barak and O. Goldreich, "Universal arguments and their applications" *SICOMP*, Volume 38, Issue 5, pages 1661–1694, 2008. Extended abstract in *17th CCC*, 2002.

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

[81] 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.

[82] 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.

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

[84] M. Bellare and O. Goldreich, "On Probabilistic versus Deterministic Provers in the Definition of Proofs Of Knowledge", *ECCC*, TR06-136, 2006.

[85] M. Bellare, O. Goldreich, and S. Goldwasser, "Incremental Hashing and Signatures", *Advances in Cryptology – Crypto '94 (Proceedings)*, Lecture Note in Computer Science (839) Springer Verlag, pp. 216–233, 1994.

[86] M. Bellare, O. Goldreich, and S. Goldwasser, "Incremental Cryptography and Application to Virus Protection", extended abstract in *27th STOC*, 1995.

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

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

[89] M. Ben-Or, R. Canetti, and O. Goldreich, "Asynchronous Secure Computation", extended abstract in *25th STOC*, 1993.

[90] M. Ben-Or, 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.

[91] 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. Extended abstract in the proceedings of *12th ICALP*, 1985.

[92] Z. Brakerski and O. Goldreich, "From absolute distinguishability to positive distinguishability", ECCC, Report TR09-031, Apr. 2009

[93] R. Canetti, U. Feige, O. Goldreich and M. Naor, "Adaptively Secure Multi-party Computation", extended abstract in *28th STOC*, 1996.

[94] R. Canetti, O. Goldreich, S. Goldwasser, and S. Micali. "Resettable Zero-Knowledge", *32th STOC*, pages 235–244, 2000.

[95] R. Canetti, O. Goldreich and S. Halevi, "The Random Oracle Methodology, Revisited", *Jour. of the ACM*, Vol. 51 (4), pages 557–594, July 2004. Extended abstract in *30th STOC*, pp. 209–218, 1998.

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

[97] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, "Private Information Retrieval", *JACM*, Vol. 45, No. 6, pages 965–982, November 1998. Extended abstract in *36th FOCS*, 1995.

[98] I. Damgard, O. Goldreich, and A. Wigderson, "Hashing Functions can Simplify Zero-Knowledge Protocol Design (too)", BRICS Techniacl Report, 1994. Appeared in *Crypto95* jointly with T. Okamoto under the title "Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs".

[99] A. De Santis, G. Di Crescenzo, O. Goldreich, and G. Persiano, "The Graph Clustering Problem has a Perfect Zero-Knowledge Proof", *IPL*, Vol. 69, pp. 201–206, 1999. (Superseeds *ECCC* TR96-054, by O.G., November 1996.)

[100] 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.

[101] S. Even and O. Goldreich, "On The Security of Multi-Party Ping-Pong Protocols", extended abstract in the proceedings of *24th FOCS*, pp. 34–39, 1983.

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

[103] 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. Extended abstract in the proceedings of *Crypto82*.

[104] S. Even, O. Goldreich, and S. Micali, "On-line/Off-line Digital signatures", *Journal of Cryptology*, Vol. 9, No. 1, 1996, pp. 35–67. Preliminary version in the proceedings of *Crypto89*.

[105] 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.

[106] 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)*, pp. 58–72, 1986.

[107] D. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev, "More Constructions of Lossy and Correlation-Secure Trapdoor Functions", in the proceedings of *13th PKC*, Springer LNCS, Vol. 6056, pages 279–295, 2010.

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

[109] 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.

[110] 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.

[111] O. Goldreich, "Towards a Theory of Software Protection and Simulation by Oblivious RAMs", *Proc. of the 19th ACM Symp. on Theory of Computing*, pp. 182–194, 1987.

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

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

[114] O. Goldreich. "The GGM Construction does NOT yield Correlation Intractable Function Ensembles", *Cryptology ePrint Archive*, Report 2002/110, 2002.

[115] O. Goldreich, "On Expected Probabilistic Polynomial-Time Adversaries: A suggestion for restricted definitions and their benefits", *Journal of Cryptology*, Volume 23, Issue 1, pages 1–36, 2010. Extended abstract in the *4th Theory of Cryptography Conference*, Springer LNCS, Vol. 4392, pages 174–193, 2007.

[116] O. Goldreich, S. Goldwasser, and S. Halevi, Collision-Free Hashing from Lattice Problems, *ECCC*, TR96-042, 1996.

[117] O. Goldreich, S. Goldwasser, and S. Halevi, Public-Key Cryptosystems from Lattice Reduction Problems, in *Crypto97*, 1997.

[118] O. Goldreich, S. Goldwasser, and S. Halevi, Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem, in *Crypto97*, 1997.

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

[120] O. Goldreich, S. Goldwasser and S. Micali, "On the Cryptographic Applications of Random Functions", in *Advances in Cryptology: Proceedings of Crypto84*, pp. 276–288, 1985.

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

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

[123] 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. Extended abstract in proceedings of the *17th ICALP*, 1990.

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

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

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

[127] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs". *JACM*, Vol. 38, No. 1, pp. 691–729, 1991. Extended abstract in *27th FOCS*, 1986.

[128] 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*, pp. 218–229, 1987.

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

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

[131] O. Goldreich and R. Rothblum, "Enhancements of Trapdoor Permutations",

[132] O. Goldreich, and A. Sahai and S. Vadhan. "Honest-Verifier Statistical Zero-Knowledge equals general Statistical Zero-Knowledge", in *30th STOC*, pp. 399–408, 1998.

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

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

[135] 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.

1.3 Other Areas of the Theory of Computation

Distributed Computing. Throughout the years, I have maintained some interest in the area of distributed computing. In particular, I am familiar and have worked on problems in various models including static and dynamic asynchronous networks, fault-tolerant distributed computing, and radio networks. My contributions include

- Lower bounds on the message complexity of broadcast and related tasks in asynchronous networks [137];
- Investigation of the deterministic and randomized round-complexity of broadcast in radio networks [138,139];
- Enhancement of fast randomized Byzantine Agreement algorithms so that they always terminate [148];
- Initiating a quantitative approach to the analysis of dynamic networks [136];
- Construction of a randomized reliable channel over a highly unreliable media [146]; and
- Investigations of the message complexity of computations in the presence of link failures [152, 153, 154].

Average-case complexity. I consider the theory of average case complexity initiated by Levin to be fundamental. This theory provides a framework for investigating the behaviour of algorithms and problems under *any* "reasonable" input distribution. In [140], an attempt was made to further develop and strengthen this approach. In particular, the class of "reasonable" distributions has been extended to all distributions for which there exists efficient sampling algorithms, and a completeness result for the new class has been presented. (Fortunately, Impagliazzo and Levin subsequently showed a general method for translating completeness results from the original framework to the new one, thus unifying the two frameworks.) Furthermore, [140] also contained a reduction of search to decision problems, abolishing the fear that two separate theories will need to be investigated.

A Theory of Goal-Oriented Communication. I have contributed to the formalization of the general theory of goal-oriented communication, initiated by Juba and Sudan [42].

Computational Learning Theory. My works in this area include [151, 149, 142]. In particular, in [142] we introduced a new measure of learning complexity called *computational sample complexity* that represents the number of examples sufficient for *polynomial time* learning with respect to a fixed distribution. We then show concept classes that (under standard cryptographic assumptions) possess arbitrary sized gaps between their standard (information-theoretic) sample complexity and their computational sample complexity.

Coding Theory. Some of my works deal explicitly or implicitly with *list-decoding* of certain error-correcting codes. Specifically, [47] may be viewed as providing such a procedure for the Hadamard code, and [151] as dealing with Reed–Muller codes. In [150], a list-decoding algorithm is presented for the Chinese Remainder code. Locally decodable codes and locally testable codes are studied in [147] and [67], respectively.

Miscelaneous. I have some research experience in parallel computation (i.e., a parallel algorithm for integer GCD computation [141]), and in combinatorics (motivated by algorithmic problems as in [145, 18]). Finally, as many theoretical computer scientist, I've proven several NP-completeness results (e.g. for problems in permutation groups [143], for several network testing problems [144], and for a problem concerning games [155]).

Publications in this area

[136] 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.

[137] 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.

[138] R. Bar-Yehuda, O. Goldreich, and 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.

[139] 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.

[140] 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. Extended abstract in the proceedings of *21th STOC*, 1989.

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

[142] S. Decatur, O. Goldreich, and D. Ron, "Computational Sample Complexity", *SICOMP*, Vol. 29, Nr. 3, pages 854–879, 1999. Extended abstract in the proceedings of *10th COLT*, 1997.

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

[144] 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.

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

[146] 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)*, pp. 85-102, 1989.

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

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

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

[150] O. Goldreich, D. Ron and M. Sudan, "Chinese Remaindering with Errors", *IEEE Transactions on Information Theory*, Vol. 46, No. 4, July 2000, pages 1330–1338. Extended abstract in *31st STOC*, pages 225–234, 1999.

[151] O. Goldreich, R. Rubinfeld and M. Sudan, "Learning Polynomials with Queries: the Highly Noisy Case", *SIAM Journal on Discrete Mathematics*, Vol. 13, No. 4, pages 535–570, 2000. Extended abstract in *36th FOCS*, 1995.

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

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

[154] O. Goldreich and D. Sneh, "On the Complexity of Global Computation in the Presence of Link Failures: the case of Unidirectional Faults", *10th ACM Symp. on Principles of Distributed Computing (PODC)*, 1991.

Unpublished manuscripts in this area (cited in literature)

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

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.

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

[N7] "Foundations of Cryptography – Class Notes", Computer Science Dept., Technion, Spring 1989, 184 pages.

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

[N8] "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.)

[N9] "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.)

[N10] "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 [B12]. Available from my web-page.)

[N11] "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.)

[N12] "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 [B10] 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.

Technical surveys of single topics:

[S22] "Three XOR-Lemmas – An Exposition", *ECCC*, TR95-056, 1995.

[S23] "A Sample of Samplers – A Computational Perspective on Sampling", *ECCC*, TR97-020, May 1997.

[S24] "Notes on Levin's Theory of Average-Case Complexity", *ECCC*, TR97-058, 1997.

[S25] "On Security Preserving Reductions – Revised Terminology", *Cryptology ePrint Archive*, Report 2000/001, 2000.

[S26] "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.

3 Graduate Student Supervision

3.1 Graduate students completed D.Sc.

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 research scientist at IBM Research Division, Hawthorne, NJ, USA.

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 CS 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 CS 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 CS 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.

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.

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

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

3.2 Graduate students working towards D.Sc.

D10 Ron Rothblum. Interested in Cryptography.

3.3 Graduate students 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 studies towards a PhD at Weizmann Institute.]

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.) [Gilad studies towards a PhD at Tel-Aviv University.]

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.)

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

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.]

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 an Assistant Professor of Computer Science and Engineering at the Pennsylvania State 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.

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):

- **Complexity Theory**
  - 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
  - *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

- *Fellow of the International Association for Cryptologic Research*, 2009.
- Member of the *TCS Chair Professor Team*, Tsinghua University, since 2007.
- *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

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

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.

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

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

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

11 Public Professional Activities

11.1 Organization of Conferences and Workshops

Organization of Workshops:

- Co-organizer of the *Complexity Theory Meeting*, November 1996, November 1998, November 2000, April 2003, June 2005, June 2007, and November 2009, Oberwolfach, Germany.
- Co-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 Computer Science* (*ICS*), since being founded (in 2009).
- Member of the Steering Committee of the *Theory of Cryptography Conference* (*TCC*), since being founded (in 2003).

  Chair since Spring 2005.
- 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 *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) and *Random'06* (Vol. 17, Nr. 1, 2008).
- Since Aug. 1999: 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/`.
- 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-techncal publications address various aspects of the relevant research community and are viewed as service to that community.

- An essay "On the status of intellectual values in TOC" (reporting a sociological study and presenting opinions), Nov 2011.
- 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 Research Grants

12.1 Active

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

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

12.2 Past

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

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

- *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$.

13 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).