Research Statement

Oded Goldreich

February 1996

1 Research Experience

My most important contributions to theoretical computer science are in the areas of computational complexity and cryptography. More specifically, 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*), cryptography (e.g., *zero-knowledge* and *fault-tolerant protocols*), and distributed computing.

1.1 Randomized Computations

In recent years, randomness has become 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, 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.

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, which 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 decade.

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, I was able to prove that any one-way function of the form $f(x,r) = (f'(x), r)$ has a hard-core predicate [20]. This result played an important role in further development 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 previous results concerning specific functions of Blum and Micali, and Alexi, Chor, Schnorr and myself [1]. Put in more general terms, the result in [20] asserts that the complexity of any search problem is related to the complexity of answering "random (linear) queries" concerning the solution.

Getting back to [1], it is worthwhile to note that this work, which demonstrates a hardcore for the RSA and Rabin functions, still offers the most efficient pseudorandom generator based on the intractability of factoring.

Another contribution to the construction of pseudorandom generators is presented in [19]. This work contains a construction of pseudorandom generators based on any "regular" function. (Loosely speaking, a function f is called regular if each point in its range has the same number of preimages.) The construction used in [19] utilizes *hash functions* in order to preserve the difficulty of successive iterations of a (regular) one-way function. Traces of this paradigm can be seem in many subsequent works in the area.

The theory of pseudorandomness has been extended to functions by Goldwasser, Micali and myself [16]. In particular, it has been shown how to construct pseudorandom functions, using an arbitrary pseudorandom (bit) generator. This means that a black box which has only k secret bits of storage can implement a function from k bit strings to k bit strings, which cannot be distinguished from a random function by any poly(k)-time observer which can "query" the function on arguments of his choice.

Other works of mine in the area of pseudorandomness include [18, 15, 26, 17, 21, 22]. In particular, in [15] I've shown that two efficiently sampleable distributions which are statistically different can be computational indistinguishable only if one-way functions exist. In [17] 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.

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 which 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 [11, 9, 2, 13]. 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, [2] contains three simple constructions of small sample spaces which are almost unbiased, and [13] 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 [25], 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. It is stressed that the size of the family does not depend on the size of the domain on which the functions operate.

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 every 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 [9, 10]. In [10], Chor and myself introduce and investigate *probability bounded* sources of randomness which 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 turned out to be very central to subsequent developments in this area.

The use of random sources in algorithms is a major motivation for statistical tests, which may be thought of as "program checkers" for devices producing random outputs. A systematic approach to statistical tests has been recently initiated by Blum and myself [5].

Probabilistic Proof Systems

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 [4], 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.

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 [55] it was proved that this generalization is indeed essential for the (non-trivial) existence of zero-knowledge proofs. Also, 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 (that is not known to be in $\mathcal{NP}$) has an interactive proof system [53]. Alas, the focus of that paper is on the zero-knowledge aspects of interactive proofs – see next section.

More refined studies of the role of randomness in interactive proof systems were the subject of [14, 3]. In [14], it is shown that the error probability in the completeness condition of interactive proof systems is unessential. In [3] 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.

In [8], interactive proofs were used to present a dramatic contradiction to the "classic" Random Oracle Hypothesis. In contradiction to co$\mathcal{NP} \subseteq \mathcal{IP}$, it was shown that, *relative to a random oracle*, co$\mathcal{NP}$ is not contained in $\mathcal{IP}$.

A fundamental complexity measure associated to interactive proof systems is their knowledge complexity. This measure was suggested by Goldwasser, Micali and Rackoff, yet without satisfactory definition (for the case where complexity is greater than zero). In [24], two satisfactory definitions were presented and shown equivalent up to a constant. In [23], 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.

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 [10], 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 [7].

Publications in this area

[1] 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 proceedings of *25th FOCS*, 1984.

[2] 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.

[3] 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.

[4] M. Bellare, O. Goldreich and M. Sudan, "Free Bits and Non-Approximability", *ECCC*, TR95-024, 1995. Extended abstract in *36th FOCS*, 1995.

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

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

[7] 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.

[8] 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.

[9] 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.

[10] 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 proceedings of *26th FOCS*, 1985.

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

[12] 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.

[13] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Veličković, "Approximations of General Independent Distributions", extended abstract in *24th STOC*, 1992.

[14] 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 proceedings of *28th FOCS*, 1987.

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

[16] 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 proceedings of *25th FOCS*, 1984.

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

[18] O. Goldreich and J. Hastad, "On the Message Complexity of Interactive Proof Systems", *ECCC*, TR96-018, 1996.

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

[20] 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 proceedings of *29th FOCS*, 1988.

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

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

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

[24] O. Goldreich, R. Ostrovsky and E. Petrank, "Knowledge Complexity and Computational Complexity", extended abstract in the proceedings of *26th STOC*, 1994.

[25] O. Goldreich and E. Petrank, "Quantifying Knowledge Complexity", extended abstract in *32nd FOCS*, 1991.

[26] O. Goldreich and A. Wigderson, "Tiny Families of Functions with Random Properties", extended abstract in the proceedings of *26th STOC*, 1994.

Unpublished manuscripts in this area (cited in literature)

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

1.2 Cryptography and related areas

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. Cryptography today not only has its own merits but also sheds light on fundamental issues concerning computation such as randomization, knowledge and interaction.

Zero-Knowledge and Protocol Design

My most important contribution to the field is the work on zero-knowledge, coauthored by Micali and Wigderson [53]. 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.

The dramatic effect of the above work on the design of cryptographic protocols is demonstrated in another paper of the same authors [54]. Using additional ideas, it is shown that any *protocol problem* can be solved. Specifically, for every n-ary (computable) function f, we construct a fault-tolerant protocol computing f. 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 "simulates" a trusted party in an environment in which no party can be trusted (and furthermore any minority may be malicious). Furthermore, 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 [54] has also inspired the development and study of cryptographic protocols in the private channel model (cf., work by Ben-Or, Goldwasser and Wigderson).

Other works of mine in the area of zero-knowledge proof systems include [55, 52, 51, 47, 50, 27, 35]. A joint 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 [55, 47, 51] various formulations of zero-knowledge are suggested and investigated and certain properties of proof systems are demonstrated essential to the zero-knowledge property.

Other works of mine in the area of cryptographic protocols include [56, 30, 33]. In [56] it is shown that general multi-party computation reduces to a very simple two-party computation (of a two-bit function). In [30] the scope of multi-party computation is extended to the asynchronous setting, whereas [33] deals with adaptive/dynamic adversaries (in both the private channel and the computational models). Early works on testing and designing simple protocols appear in [37, 43, 41, 39, 44, 32, 42].

Pseudorandomness

Pseudorandom generators, surveyed in the previous section, are very important to cryptography. In particular, pseudorandom generators yield private-key encryption schemes. Several cryptographic applications (e.g., message authentication) of pseudorandom functions were described in [49]. Pseudorandom functions were also essential to the results in [46, 45].

Results from cryptography (and in particular pseudorandom functions [16]) were used to derive many of the impossibility results in the area of machine learning.

New Topics in Cryptography

The notion of incremental cryptography was introduced and developed in [28, 29]. The aim of this approach is to design cryptographic algorithms 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 which 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 [34], we consider the problem of querying a duplicated database so that none of the individual copies can know which record has been required by the user. We have obtained several efficient schemes for this problem.

In [46], I have initiated a theoretical treatment of software protection.

Other Topics in Cryptography

I have also worked on the "classical" problems of cryptography, namely encryption [47] and signatures [45, 40]. In particular, in [40] the notion of an On-line/Off-line Signature Scheme is presented and instantiated.

Publications in this area

[28] 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.

[29] 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.

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

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

[32] 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.

[33] 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.

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

[35] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, "Private Information Retrieval", extended abstract in *36th FOCS*, 1995.

[36] 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".

[37] 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.

[38] 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.

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

[40] 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*.

[41] 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*.

[42] 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.

[43] 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.

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

[45] 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.

[46] 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.

[47] 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.

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

[49] O. Goldreich, S. Goldwasser, and N. Linial, "Fault-tolerant Computations without Assumptions: the Two-party Case", extended abstract in *32nd FOCS*, 1991.

[50] 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.

[51] O. Goldreich, and A. Kahan, "How to Construct Constant-Round Zero-Knowledge Interactive Proofs for NP", To appear in *Journal of Cryptology*,

[52] 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.

[53] 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.

[54] 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 proceedings of *27th FOCS*, 1986.

[55] 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.

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

[57] 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 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 [59];
- Investigation of the deterministic and randomized round-complexity of broadcast in radio networks [60,61];
- Initiating a quantitative approach to the analysis of dynamic networks [58];
- Enhancement of fast randomized Byzantine Agreement algorithms so that they always terminate [63];
- Construction of a randomized reliable channel over a highly unreliable media [62]; and
- Investigations of the message complexity of computations in the presence of link failures [64, 65, 66].

Publications in this area

[58] 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.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.

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

[65] 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.

[66] 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.

1.4 Other Areas of Complexity Theory

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 [67], 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, [67] also contained a reduction of search to decision problems, abolishing the fear that two separate theories will need to be investigated.

In [72], we study the problem of reconstructing a function when given access to an oracle (for it) which is very rarely correct. We have obtained such a procedure for the case where the function is an (unknown) low-degree (multi-variant) polynomial over a large finite field.

I have some research experience in parallel computation (i.e., a parallel algorithm for integer GCD computation [68]), and in combinatorics (motivated by algorithmic problems as in [71, 9]). Finally, as many theoretical computer scientist, I've proven several NP-completeness results (e.g. for problems in permutation groups [69], for several network testing problems [70], and for a problem concerning games [73]).

Publications in this area

[67] 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.

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

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

[70] 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.

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

[72] O. Goldreich, R. Rubinfeld and M. Sudan, "Learning Polynomials with Queries: the Highly Noisy Case", extended abstract in *36th FOCS*, 1995.

Unpublished manuscripts in this area (cited in literature)

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