Work and Publications

Oded Goldreich

June 1, 2002

Preface

Most work dating to after 1992 are available in PostScript from the webpage

`http://www.wisdom.weizmann.ac.il/~oded/papers.html`

Abstracts: Some of the original abstracts are reproduced almost without change and some with minor revision. The former cases are indicated by v.o., whereas the latter cases are indicated by rev.

Common abbreviations (for the publication items) include:

CCC: Annual IEEE Conference on Computational Complexity.

COLT: Annual ACM Workshop on Computational Learning Theory.

FOCS: Annual IEEE Symposium on Foundation of Computer Science.

ICALP: International Colloquium on Automata Languages and Programming.

PODC: Annual ACM Symposium Principles of Distributed Computing.

STOC: Annual ACM Symposium on Theory of Computing.

ECCC and ePrint are unreferred depositories dedicated to Complexity Theory and Cryptography, respectively.

Graduate School (1981–83)

1 The Minimum Length Generator Sequence is NP-Hard

Two computational problems regarding groups are shown to be NP-hard. In one, given a set of generators and a target element in the group formed by them, it is required to find the shortest sequence of generators that when composed yield the target.

Comments: Authored by S. Even and O. Goldreich. (Indeed, this was my first paper.) Appeared in

- *Journal of Algorithms*, vol. 2, pp. 311–313, 1981.

2 DES-Like Functions Can Generate the Alternating Group

Comments: Authored by S. Even and O. Goldreich. Appeared in

- *IEEE Trans. on Inform. Theory*, Vol. IT-29, No. 6, pp. 863–865, 1983.

3 On the NP-Completeness of Certain Network-Testing Problems

Comments: Authored by S. Even, O. Goldreich, S. Moran and P. Tong. (This was my M.Sc. Thesis.) Appeared in

- *Networks*, Vol. 14, No. 1, pp. 1–24, 1984.

4 A Randomized Protocol for Signing Contracts

In retrospect, the most important contribution of this work is in introducing and studying an abstract notion of Oblivious Transfer. Specifically, the notion of 1-out-of-2 Oblivious Transfer is introduced, the plausibility of implementing it is demonstated, and so is its applicability.

Comments: Authored by S. Even, O. Goldreich and A. Lempel. Appeared in

- *Proceedings of Crypto82*, Plenum Press, pages 205–210, 1983.
- *Comm. of the ACM*, Vol. 28, No. 6, pp. 637–647, 1985.

5 On The Security of Multi-Party Ping-Pong Protocols

This work refers to a restricted notion of insecurity (i.e., breakability under a syntactically restricted type of atttacks) and to restricted classes of protocols. The computational task of testing whether or not such protocols are insecurity is studied, and is shown to be undecidable for one of the classes and NP-hard for another.

Abstract (v.o.): This paper is concerned with the model for security of cryptographic protocols suggested by Dolev and Yao. The Dolev and Yao model deals with a restricted class of protocols, known as *Two-Party Ping-Pong Protocols*. In such a protocol, messages are exchanged in a memoryless manner. That is, the message sent by each party results from applying a predetermined operator to the message he has received.
The Dolev and Yao model is presented, generalized in various directions and the affect of these generalizations is extensively studied. First, the model is trivially generalized to deal with multi-party ping-pong protocols. However, the problems which arise from this generalization are very far from being trivial. In particular, it is no longer clear how many saboteurs (adversaries) should be considered when testing the security of p-party ping-pong protocols. We demonstrate an upper bound of $3(p-2)+2$ and a lower bound of $3(p-2)+1$ on this number. Thus, for every fixed p, the security of p-party ping-pong protocols can be tested in polynomial time. In contrast, we show that testing the security of multi-party protocols (i.e. the number of participants is part of the input) is NP-Hard. A different extension of the Dolev and Yao model, obtained by allowing operators to operate on "half words", is shown to have an undecidable security problem.

Comments: Authored by S. Even and O. Goldreich. (This was the main part of my D.Sc. Thesis.) Appeared in

- *Proc. of the 24th FOCS*, pages 34–39, 1983.

6 A Simple Protocol for Signing Contracts

Comments: Authored by O. Goldreich. Appeared in

- *Proceedings of Crypto83*, Plenum Press, pages 133–136, 1984.

7 Electronic Wallet

Comments: Authored by S. Even, O. Goldreich and Y. Yacobi. Appeared in

- *Proceedings of Crypto83*, Plenum Press, pages 383–386, 1984.

8 On the Power of Cascade Ciphers

Comments: Authored by S. Even and O. Goldreich. Appeared in

- *Proceedings of Crypto83*, Plenum Press, pages 43–50, 1984.
- *ACM Trans. on Computer Systems*, Vol. 3, No. 2, pp. 108–116, 1985.

9 On Concurrent Identification Protocols

Comments: Authored by O. Goldreich. Appeared in

- *Proceedings of Eurocrypt84*, Lecture Note in Computer Science (209) Springer Verlag, pp. 387–396, 1985.

The Post-Doctoral Period (1983–86)

10 How to Construct Random Functions

This work extends the theory of pseudorandomness to functions. A collection of functions is called pseudo-random if it is infeasible to distinguish the case one is given oracle access to a function chosen uniformly

in the collection from the case one is given oracle access to a truely random function. It is shown how to construct collections of pseudorandom functions from any pseudorandom generator.

Abstract (rev.): A constructive theory of randomness for functions, based on computational complexity, is developed, and a pseudorandom function generator is presented. This generator is a deterministic polynomial-time algorithm that transforms pairs *(g,r)*, where g is any one-way permutation and r is a random k-bit string, to a polynomial-time computable function from k-bit strings to k-bit strings. Such a function (indexed by a random r) cannot be distinguished from a random function by any probabilistic polynomial-time algorithm that asks and receives the value of the function at raguments of its choice. The result has applications in cryptography, random coinstructions, and complexity theory.

Comments: Authored by O. Goldreich, S. Goldwasser and S. Micali. Appeared in

- *Proc. of the 25th FOCS*, 1984, pages 464-479.
- *Jour. of the ACM*, Vol. 33, No. 4, Oct. 1986, pp. 792–807.

11 Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle is NP-Hard

Comments: Authored by O. Goldreich.

Unpublished manuscript, July 1984.

12 The Weakest Pseudo-Random Generator Implies the Strongest One

It is shown that any pseudorandom generator that stretches its seed by only one bit can be used to construct pseudorandom generators of arbitrary strecthing functions.

Comments: Authored by O. Goldreich and S. Micali.

Unpublished manuscript, October 1984.

13 On the Number of Monochromatic and Close Beads in a Rosary

(The original motivation for this combinatorial study was the analysis of certain oracle probing techniques that emerged from the attempt to prove that the least significant bit is a hardcore of the RSA function.)

Comments: Authored by O. Goldreich. Appeared in

- *Proceedings of Eurocrypt84*, Lecture Note in Computer Science (209) Springer Verlag, pp. 127–141, 1985.
- *Discrete Mathematics*, Vol. 80, 1990, pp. 59–68.

14 RSA/Rabin Functions: Certain Parts are As Hard As the Whole

It is shown that the least significant bit is a hard-core predicate of the RSA and Rabin functions. That is, ability to guess this bit correctly from the value of the function, with non-negligible advantage, yields ability to invert the function. The proof demonstrates one fundamental advantage of certain pairwise-independent sequences over sequences of total independence.

Abstract (rev.): The RSA and Rabin functions index by a composite N are defined by raising the input to the power e (where e is relatively prime to *phi(N)*) and squaring modulo N, respectively. We prove that for both functions, the following problems are computationally equivalent (i.e., each is probabilistic polynomial-time reducible to the other):

1. Given N and the value of the function, find its preimage.
2. Given N and the value of the function, guess the value of the least-significant bit of the preimage with success probability non-negligibly bigger than *1/2*.

This equivalence implies that an adversary, given the RSA/Rabin ciphertext, cannot have a non-negligible advantage (over a coin flip) in guessing the least-significant bit of the plaintext, unless he can invert-RSA/factor. The proof technique also yields the simultaneous security of logarithmically many least-significant bits. Our results improve the efficiency of pseudo-random generators and probabilistic encryption schemes that are based on the intractability of factoring.

Comments: Authored by W. Alexi, B. Chor, O. Goldreich and C. P. Schnorr. Appeared in

- *Proc. of the 25th FOCS*, 1984, pp. 449-457.
- (partial result w/ B. Chor only), *Crypto84 (Proceedings)*, Lecture Note in Computer Science (196) Springer Verlag, pp. 303–313, 1985.
- *SIAM Jour. on Comp.*, Vol. 17, No. 2, April 1988, pp. 194–209.

15 On the Cryptographic Applications of Random Functions

It is shown that secure private-key encryption and message-authentication schemes can be constructed using a collection of pseudorandom functions. In both cases, security is with respect to adaptive chosen ciphertext (or document) attacks.

Comments: Authored by O. Goldreich, S. Goldwasser and S. Micali. Appeared in

- *Crypto84 (Proceedings)*, Lecture Note in Computer Science (196) Springer Verlag, pp. 276–288, 1985.

16 On the Power of Two–Point Based Sampling

It is shown that a sequence of pairwise-independent samples, which can be constructed based on randomness proportional to the amount required to generate two samples, can be used to approximate the average of any function defined over the corresponding domain.

Abstract (v.o.): The purpose of this note is to present a new sampling technique and to demonstrate some of its properties. The new technique consists of picking two elements at random, and deterministically generating (from them) a long sequence of pairwise independent elements. The sequence is guarantees to intersect, with high probability, any set of non-negligible density.

Comments: Authored by B. Chor and O. Goldreich. Appeared in

- *Jour. of Complexity*, Vol 5, 1989, pp. 96–106.

17 On the Complexity of Global Computation in the Presence of Link Failures – The Case of a Ring

Comments: Authored by O. Goldreich and L. Shrira. Appeared in

- *Proc. of the 5th PODC*, pp. 174–185, 1986.
- *Distributed Computing*, Vol. 5, 1991, pp. 121–131.

18 Electing a Leader in a Ring with Link Failures

Comments: Authored by O. Goldreich and L. Shrira. Appeared in

- *ACTA Informatica*, Vol. 24, pp. 79–91, 1987.

19 Unbiased Bits From Sources of Weak Randomness and Probabilistic Communication Complexity

Focusing on the min-entropy of distributions, the notion of a block-source is introduced and studied. The treatment extends previous results that may be casted as referring to blocks consisting of a single bit. Lower bounds on the randomized communication complexity of specific and random functions are derived.

Abstract (v.o.): A new model for weak random physical sources is presented. The new model strictly generalizes previous models (e.g., the Santha and Vazirani model). The sources considered output strings according to probability distributions in which *no single string is too probable.* The new model provides a fruitful viewpoint on problems studied previously as:

- *Extracting almost perfect bits from sources of weak randomness:* The question of possibility as well as of efficiency of such extraction schemes are addressed.
- *Probabilistic Communication Complexity:* It is shown that most functions have linear communication complexity in a very strong probabilistic sense.
- *Robustness of BPP* with respect to sources of weak randomness (generalizing a result of Vazirani and Vazirani).

Comments: Authored by B. Chor and O. Goldreich. Appeared in

- *Proc. of the 26th FOCS*, 1985, pp. 429-442.
- *SIAM Jour. on Comp.*, Vol. 17, No. 2, April 1988, pp. 230–261.

20 The Bit Extraction Problem or t-Resilient Functions

The question addressed is that of the possibility of extracting random bits from several bits, where a bounded number of these bits (including the choice of their identity) are controlled by an adversary and the rest are uniformly distributed. Lower and upper bounds on the number of uniformly distributed bits that can be extracted, as a function of the fraction of bits controlled by the adversary, are presented. Among the is a lower bound on the size of sample spaces for limited-independence random variables.

Comments: Authored by B. Chor, J. Friedmann, O. Goldreich, J. Hastad, S. Rudich and R. Smolansky. Appeared in

- *Proc. of the 26th FOCS*, 1985, pp. 396-407.

21 An Improved Parallel Algorithm for Integer GCD

Comments: Authored by B. Chor and O. Goldreich. Appeared in

- *Algorithmica*, 5, pp. 1–10, 1990.

22 A Fair Protocol for Signing Contracts

Comments: Authored by M. Ben-Or, O. Goldreich, S. Micali and R.L. Rivest. Appeared in

- *Proc. of the 12th ICALP*, Lecture Note in Computer Science (194) Springer Verlag, 1985, pp. 43-52.
- *IEEE Trans. on Inform. Theory*, Vol. 36, No. 1, pp. 40–46, Jan. 1990.

23 On the Security of Ping-Pong Protocols when Implemented Using the RSA

Comments: Authored by S. Even, O. Goldreich and A. Shamir. Appeared in

- *Crypto85 (Proceedings)*, Lecture Note in Computer Science (218) Springer Verlag, pp. 58–72, 1986.

24 The Bit Security of Modular Squaring given Partial Factorization of the Modulus

Comments: Authored by B. Chor, O. Goldreich, S. Goldwasser. Appeared in

- *Crypto85 (Proceedings)*, Lecture Note in Computer Science (218) Springer Verlag, pp. 448–457, 1986.

25 Two Remarks Concerning the GMR Signature Scheme

It is shown that the GMR signature scheme can be made memoryless as well as implemented in time comparable to a few RSA computations.

Comments: Authored by O. Goldreich. Appeared in

- *Crypto86 (Proceedings)*, Lecture Note in Computer Science (263) Springer Verlag, pp. 104–110, 1987.

26 Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs

This work demonstrates the wide applicability of the notion of zero-knowledge. Most importantly, using any commitment scheme, it is show how to transform any NP-proof system into a zero-knowledge interactive proof system. In addition, a perfect zero-knowledge proof is presented for Graph Isomorphism, and a constant-round interactive proof is presented for the complement set (which is not known to be in NP).

Abstract (v.o.): In this paper 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 of a language, efficiently demonstrate membership in the language without conveying any additional knowledge. All previously known zero-knowledge proofs were only for number-theoretic languages in the intersection of NP and CoNP.

Comments: Authored by O. Goldreich, S. Micali and A. Wigderson. Appeared in

- *Proc. of the 27th FOCS*, pp. 174-187, 1986.
- *Jour. of the ACM*, Vol. 38, No. 3, July 1991, pp. 691–729.

27 Towards a Theory of Software Protection and Simulation by Oblivious RAMs

The problem of hiding the memory-access sequence (of a protected CPU) is introduced and an efficient solution is provided. The heart of the solution is a randomized simulation of an arbitrary Random Access Machine (RAM) on an "oblivious RAM" (a randomized RAM in which the distribution of the memory-access sequence is independent of the actual input).

Comments: Authored by O. Goldreich. Appeared in

- *Proc. of the 19th STOC*, pp. 182-194, 1987.
- Journal version with R. Ostrovsky ("Software Protection and Simulation on Oblivious RAMs") *Jour. of the ACM*, Vol. 43, No. 3, 1996, pp. 431–473.

28 How to Play any Mental Game or a Completeness Theorem for Protocols with Honest Majority

It is shown how to securely implement that any desired multi-party functionality. Security can be guaranteed provided either a majority of the players are honest or all parties are "semi-honest" (i.e., send messages according to the protocol, but keep track of and share all intermediate results).

Abstract (rev.): We present a general theorem in the field of fault tolerant distributed computing. Following is a simplified description of a special case of this theorem. Loosely speaking, a *protocol problem* is a multi-argument function f and its *solution* is a multi-party fault-tolerant protocol having the following two properties:

1. *Correctness*: The protocol allows each party to obtain the value of the function on arguments scattered among all the parties.
2. *Privacy*: Whatever a party can efficiently compute after participating in the protocol, he can also efficiently compute from his local input and his local output.

In other words, participating in the protocol is equivalent to getting the value of the function from a trusted oracle. For example, if the function is the sum of the party's inputs, then a solution is a protocol at the end of which each party gets the sum of the inputs without gaining any additional knowledge as to how the residual sum is partitioned among his counterparts.

Assuming the existence of secure encryption functions, it will be shown that every protocol problem has a solution with complexity polynomial in the complexity of the problem. Furthermore, we present an efficient algorithm that, on input a Turing machine description of a function, outputs an efficient solution for this problem.

Comments: Authored by O. Goldreich, S. Micali and A. Wigderson. Appeared in

- *Proc. of the 19th STOC*, pp. 218-229, 1987.

29 Everything Provable is Provable in Zero-Knowledge

Using any commitment scheme, it is show how to transform any interactive proof system into a zero-knowledge interactive proof system.

Comments: Authored by Ben-Or, M., O. Goldreich, S. Goldwasser, J. Hastad, J. Kilian, S. Micali and P. Rogaway. Appeared in

- *Crypto88 (Proceedings)*, Lecture Note in Computer Science (403) Springer Verlag, pp. 37–56, 1990.

The Technion Period (1986–94)

30 On the Time-Complexity of Broadcast in Radio Networks: An Exponential Gap Between Determinism and Randomization

The complexity of broadcast in a radio network of unknown topology is considered. The model is synchronous and a processor acting as a receiver at a given communication round receives a message at that round if and only if exactly one of its neighbors transmits at that round.

Comments: Authored by R. Bar-Yehuda, O. Goldreich, A. Itai. Appeared in

- *Proc. of the 6th PODC*, 1987, pp. 98–108.
- *Journal of Computer and system Sciences*, Vol. 45, (1992), pp. 104–126.

31 Efficient Emulation of Single-Hop Radio Network with Collision Detection on Multi-Hop Radio Network with no Collision Detection

Comments: Authored by R. Bar-Yehuda, O. Goldreich, A. Itai. Appeared in

- *Distributed Computing*, Vol. 5, 1991, pp. 67–71.

32 How to Solve any Protocol Problem – An Efficiency Improvement

The main observation is that general secure multi-party computation can be reduced to 1-out-of-2 Oblivious Transfer.

Comments: Authored by O. Goldreich and R. Vainish. Appeared in

- *Crypto87 (Proceedings)*, Lecture Note in Computer Science (293) Springer Verlag, pp. 73–86, 1988.

33 On Completeness and Soundness in Interactive Proof Systems

It is shown that any interactive proof can be transformed into one with perfect completeness. In contrast, perfectly sound interactive proofs exist only for NP.

Comments: Authored by M. Furer, O. Goldreich, Y. Mansour, M. Sipser and S. Zachos. Appeared in

- *Proc. of the 28th FOCS*, pp. 449-461, 1987.
- *Advances in Computing Research: a research annual*, Vol. 5 (Randomness and Computation, S. Micali, ed.), pp. 429–442, 1989.

34 A Trade-off between Information and Communication in Broadcast Protocols

The main result is a linear lower bound on the complexity of broadcast in the standard point-to-point network model.

Comments: Authored by B. Awerbuch, O. Goldreich, D. Peleg and R. Vainish. Appeared in

- *Jour. of the ACM*, Vol. 37, No. 2, April 1990, pp. 238–256.

35 Definitions and Properties of Zero-Knowledge Proof Systems

Among the results is a proof that zero-knowledge w.r.t auxiliary-input is closed under sequential composition, and that the non-trivilaity of zero-knowledge requires that both the prover and the verifier employ randomized strategies.

Comments: Authored by O. Goldreich and Y. Oren. Appeared in

- *Journal of Cryptology*, Vol. 7, No. 1 (1994), pp. 1–32.

36 On the Existence of Pseudorandom Generators

It is shown how to construct pseudorandom generators from any regular one-way function. A key ingrediant in the construction is the use of hashing functions.

Comments: Authored by O. Goldreich, H. Krawczyk and M. Luby. Appeared in

- *Proc. of the 29th FOCS*, pp. 12-24, 1988.
- *SIAM Jour. on Comp.*, Vol. 22-6 (Dec. 1993), pp. 1163–1175.

37 A Perfect Zero-Knowledge Proof for a Decision Problem Equivalent to Discrete Logarithm

In proving that such a problem belongs to the class of problems having perfect zero-knowledge proof (PZK), this work provides addition support to the belief that the class PZK is a strict superset of BPP.

Comments: Authored by O. Goldreich and E. Kushilevitz. Appeared in

- *Crypto88 (Proceedings)*, Lecture Note in Computer Science (403) Springer Verlag, pp. 57–70, 1990.
- *Journal of Cryptology*, Vol. 6, No. 2, (1993), pp. 97–116.

38 On-line/Off-line Digital signatures

The notion of an on-line/off-line signature scheme is introduced and implemented. Such schemes are advantageous in setting where the speed of (on-line) response to signing requests is more important than (off-line) pre-processing time, which takes place before the message to be signed is presented.

Comments: Authored by S. Even, O. Goldreich and S. Micali. Appeared in

- *Crypto89 (Proceedings)*, Lecture Note in Computer Science (435) Springer Verlag, pp. 263–277, 1990.
- *Journal of Cryptology*, Vol. 9, No. 1, 1996, pp. 35–67.

39 Hard-core Predicates for any One-Way Function

It is shown that any one-way function can be slightly modify to yield a one-way function that has a simple hard-core predicate. The transformation preseves many properties of the original function (e.g., being 1-1, length preserving, etc.). Implicit in the proof is a very efficient list-decoding algorithm for the Hadamard Code.

Abstract (v.o.): A central tool in constructing pseudorandom generators, secure encryption functions, and in other areas are hard-core predicates b of functions (or permutations) f, as defined by Blum and Micali. Such hard-core predicates (i.e., $b(x)$) cannot be efficiently guessed (substantially better than 50-50) given only the value of the function (i.e., $f(x)$). Both b and f are computable in polynomial time.
Yao transforms any one-way function f into a more complicated one, F, which has a hard-core predicate. The construction applies the original f to many small pieces of the input to F just to get one hard-core bit. The security of this bit may be smaller than any constant positive power of the security of f. In fact, for inputs (to F) of practical size, the pieces effected by f are so small that f can be inverted (and the "hard-core" bit computed) by exhaustive search.
In this paper we show that every one-way function, padded to the form $f(p,x)= (p,g(x))$, where p has length equal to that of x, has by itself a hard-core predicate of the same (within a polynomial) security. Namely, we prove a conjecture of Levin that the scalar product of boolean vectors p and x is a hard-core of every one-way function $f(p,x) = (p,g(x))$. The result extends to multiple (up to the logarithm of security) such bits and to any distribution on the x's for which f is hard to invert.

Comments: Authored by O. Goldreich and L.A. Levin. Appeared in

- *Proc. of the 21st ACM Symp. on Theory of Computing (STOC)*, pp. 25-32, 1989.

40 On the Theory of Average Case Complexity

This paper takes the next step in developing the theory of average case complexity initiated by Levin, by investigating basic computational questions such as the equivalence of search and decision problems in the context of average case complexity. In addition, we consider average case complexity with respect to efficiently sampleable distributions (rather than distributions with an efficiently computable accomulative function as considered by Levin).

Comments: Authored by S. Ben-David, B. Chor, O. Goldreich and M. Luby. Appeared in

- *Proc. of the 21st STOC*, pp. 204-216, 1989.
- *Journal of Computer and system Sciences*, Vol. 44, No. 2, April 1992, pp. 193–219.

41 The Best of Both Worlds: Guaranteeing Termination in Fast Randomized Byzantine Agreement Protocols

It is shown how to transform certain randomized Byzantine Agreement protocols to ones that always terminate, while preserving their expected (constant) running-time.

Comments: Authored by O. Goldreich and E. Petrank. Appeared in

- *IPL*, Vol. 36, October 1990, pp. 45–49.

42 On the Composition of Zero-Knowledge Proof Systems

It is shown that the basic (or vanilla) definition of zero-knowledge is not closed under sequential composition, whereas none of the known notions is closed under parallel composition. Furthermore, it is shown that constant-round public-coin protocols (of negligible error) cannot be proven zero-knowledge via black-box simulators.

Comments: Authored by O. Goldreich and H. Krawczyk. Appeared in

- *Proc. of the 17th ICALP*, Lecture Notes in Computer Science, Vol. 443, Springer Verlag, pp. 268–282, 1990.
- *SIAM Jour. on Comp.*, Vol. 25, No. 1, February 1996, pp. 169–192.

43 A Note on Computational Indistinguishability

It is shown that the existence of two sampleable distributions that are computationally indistinguishable but statistically far apart, implies the existence of pseudorandom generators.

Comments: Authored by O. Goldreich. Appeared in

- *IPL*, Vol. 34, pp. 277–281, May 1990.

44 Quantifying Knowledge Complexity

This paper introduces several measures of the *amount of knowledge gained via interaction*, and investigates the relations among them.

Comments: Authored by O. Goldreich and E. Petrank. Appeared in

- *Proc. of the 32nd FOCS*, pp. 59–68, 1991.
- *Computational Complexity*, Vol. 8, pages 50–98, 1999.

45 On Sparse Pseudorandom Ensembles

Comments: Authored by O. Goldreich and H. Krawczyk. Appeared in

- *Crypto89 (Proceedings)*, Lecture Note in Computer Science (435) Springer Verlag, pp. 113–127, 1990.
- *Random Structures and Algorithms*, Vol. 3, No. 2, (1992), pp. 163–174.

46 How to Construct Constant-Round Zero-Knowledge Proof Systems for NP

(One key ingrediant is solving a technical problem that arises in the simulation of a natural protocol.)

Comments: Authored by O. Goldreich and A. Kahan. Appeared in

- *Journal of Cryptology*, Vol. 9, No. 2, 1996, pp. 167–189.

47 Source to Destination Communication in the Presence of Faults

Comments: Authored by O. Goldreich, A. Herzberg and Y. Mansour. Appeared in

- *Proc. of the 8th PODC*, 1989, pp. 85–102.

48 A Uniform Complexity Treatment of Encryption and Zero-Knowledge

This paper presents definitions that refer to the infeasiblity of finding an instance for which the security guarantee fails, whereas previous definitions referred to the non-existence of such instances. It is shown that such secure schemes can be constructed under uniform-complexity assumptions, rather than under non-uniform ones.

Comments: Authored by O. Goldreich. Appeared in

- *Journal of Cryptology*, Vol. 6, No. 1, (1993), pp. 21–53.

49 A Quantitative Approach to Dynamic Networks

The core of this approach is in quantifying the reliablity (or operational-period) of links at various times, and analyzing protocol performance w.r.t the reliability of the links. The advantage of the quantitative approach is demonstrated in the analysis of a natural broadcast protocol.

Comments: Authored by B. Awerbuch, O. Goldreich and A. Herzberg. Appeared in

- *Proc. of the 9th PODC*, pp. 189–204, 1990.

50 Security Preserving Amplification of Hardness

It is shown how to transform weak one-way permutations into strong one-way permutations, while increasing the length of the argument only by a constant factor. This improves over Yao's construction that blows up the length by a factor inversely proportional to the fraction on which the original permutation is hard to invert. The construction consists of interating the original permutation, while interleaving succesive iterations with moves on an adequate expander graph.

Comments: Authored by O. Goldreich, R. Impagliazzo, L.A. Levin, R. Venkatesan and D. Zuckerman. Appeared in

- *Proc. of the 31st FOCS*, pp. 318–326, 1990.

51 Simple Constructions of Almost k-wise Independent Random Variables

Three simple constructions of small bias sample spaces are presented. The size of the sample space is quadratic in the length of the desired sequence and the inverse of the desired bias.

Comments: Authored by N. Alon, O. Goldreich, J. Hastad and R. Peralta. Appeared in

- *Proc. of the 31st FOCS*, pp. 544–553, 1990.
- *Journal of Random structures and Algorithms*, Vol. 3, No. 3, (1992), pp. 289–304.

52 Bounds on Tradeoffs between Randomness and Communication Complexity

Comments: Authored by R. Canetti and O. Goldreich. Appeared in

- *Proc. of the 31st FOCS*, pp. 766–775, 1990.
- *Computational Complexity*, Vol. 3 (1993), pp. 141–167.

53 Randomness in Interactive Proofs

A key contribution of this paper is an algorithm for estimating the average of (bounded) functions. The algorithm is optimal up-to a constant factor both in its randomness and query complexity. It consists of taking the median value of a sequence of values, where the values are the averages over pairwise-independent sub-samples, and the sub-samples are generated by a random walk on an expander graph.

Comments: Authored by M. Bellare, O. Goldreich and S. Goldwasser. Appeared in

- *Proc. of the 31st FOCS*, pp. 563–572, 1990.
- *Computational Complexity*, Vol. 4, No. 4 (1993), pp. 319–354.

54 The Random Oracle Hypothesis is False

It is shown that *relative to a random oracle*, coNP is not contained in IP. Combined with the (non-relativizing) containment of coNP in IP (proved by Lund, Fortnow, Karloff and Nisan) this yields a dramatic refutation of the Random Oracle Hypothesis.

Comments: Authored by R. Chang, B. Chor, O. Goldreich, J. Hartmanis, J. Hastad, D. Ranjan and P. Rohatgi. Appeared in

- *JCSS*, Vol. 49, No. 1 (1994), pp. 24–39.

55 Fault-tolerant Computations without Assumptions: the Two-party Case

In retrospect, the most intesresting contributions of this work are two-party and multi-party fault-tolerant protocols for sampling in a predetermined universe. Specifically, in the two-party protocol, for any subset of the universe, no party may force the outcome to reside in this subset with probability greater than the square root of the density of this subset.

Comments: Authored by O. Goldreich, S. Goldwasser and N. Linial. Appeared in

- *Proc. of the 32nd FOCS*, pp. 447–457, 1991.
- *SIAM Jour. on Comp.*, Volume 27, Number 2, April 1998, Pages 506–544.

56 Approximations of General Independent Distributions

This work presents efficient constructions of small probability spaces that approximate the joint distribution of general (independent) random variables. This improves over previous results, which focused on the special case of identical, uniformly distributed random variables.

Comments: Authored by G. Even, O. Goldreich, M. Luby, N. Nisan and B. Velickovic. Appeared in

- *Proc. of the STOC*, pp. 10–16, 1992.
- *Random Structures and Algorithms*, Vol. 13, No. 1, pp. 1–16, Aug. 1998.

57 Towards a Computational Theory of Statistical Tests

This work initiates a computational theory of statistical tests, which are algorithms that reject only a negligible fraction of the possible strings. The work studies the existence and efficiency of universal statistical tests for various classes of statistical tests, where a test is called universal for a class if it rejects all (but finitely many) of the strings rejected by any statistical test in the class.

Comments: Authored by M. Blum and O. Goldreich. Appeared in

- *Proc. of the 33rd FOCS*, pp. 406-416, 1992.

58 On the Complexity of Global Computation in the Presence of Link Failures: the case of Unidirectional Faults

Comments: Authored by O. Goldreich and D. Sneh. Appeared in

- *Proc. of the 11th PODC*, pp. 103–111, 1992.

59 On Defining Proofs of Knowledge

This work provides a comprehensive definitional treatment of the intruiging concept of a proof of knowledge. Special attention is placed on providing a definition that can be actually used for the intended applications.

Comments: Authored by M. Bellare and O. Goldreich. Appeared in

- *Crypto92 (Proceedings)*, Lecture Note in Computer Science (740) Springer Verlag, pp. 390–420, 1993.

60 Proofs of Computational Ability

Extending the definition of a proof of knowledge, this work provides a definition of the concept of a proof of computational ability.

Comments: Authored by M. Bellare and O. Goldreich. (Unpublished manuscript, 1992.) See also *Theory of Cryptography Library*, record Arc-03.

61 Asynchronous Secure Computation

Comments: Authored by M. Ben-Or, R. Canetti and O. Goldreich. Appeared in

- *Proc. of the 25th STOC*, pp. 52-61, 1993.

62 Lower Bounds for Sampling Algorithms for Estimating the Average

This work provides lower bounds on the randomness and query complexities of algorithms for estimating the average of (bounded) functions.

Comments: Authored by R. Canetti, G. Even and O. Goldreich. Appeared in

- *IPL*, Vol. 53, pp. 17–25, 1995.

63 Tiny Families of Functions with Random Properties: A Quality–Size Trade–off for Hashing

This work presents families of hashing functions that posses two random properties of universal hashing functions; specifically, the extraction and mixing properties. The size of these families is polynomially related the the parameter that determines the quality of these properties.

Comments: Authored by O. Goldreich and A. Wigderson. Appeared in

- *Proc. of the 26th STOC*, pp. 574-583, 1994.
- *Journal of Random structures and Algorithms*, Volume 11, Number 4, December 1997, pages 315–343.

64 Knowledge Complexity and Computational Complexity

The main result is that any set having an interactive proof of logarithmic statistical-knowledge complexity, can be recognized in probabilistic polynomial-time with the help of an NP-orcale.

Comments: Authored by O. Goldreich, R. Ostrovsky and E. Petrank. Appeared in

- *Proc. of the 26th STOC*, pp. 534-543, 1994.
- *SIAM Jour. on Comp.*, Volume 27, Number 4, pp. 1116–1141, August 1998.

The First 1.5 Years at Weizmann (1994–96)

65 Incremental Cryptography: the Case of Hashing and Signing

Comments: Authored by M. Bellare, O. Goldreich and S. Goldwasser. Appeared in

- *Crypto94 (Proceedings)*, Lecture Note in Computer Science (839) Springer Verlag, pp. 216–233, 1994.

66 A Combinatorial Consistency Lemma with application to the PCP Theorem

The lemma asserts conditions under which one may test by a constant number of queries whether a function applied to a sequence of arguments is consistent with any function that is applied to a single argument.

Comments: Authored by O. Goldreich and S. Safra. Appeared in

- *Random97*, Springer LNCS, Vol. 1269, pp. 67–84.
- *SIAM Jour. on Comp.*, Volume 29, Number 4, pages 1132–1154, 1999.

67 Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs

The main result in this paper is a transformation of public-coin constant-round protocols that are zero-knowledge with respect to the honest verifier into protocols that are zero-knowledge in the general sense. The core of the transformation is a simple random selection protocol, which is based on hashing functions (rather than on a multi-round "interactive hashing sub-protocol").

Comments: Authored by I. Damgard, O. Goldreich, T. Okamoto and A. Wigderson. Appeared in

- *Crypto95 (Proceedings)*, Lecture Note in Computer Science (963) Springer Verlag, pp. 325–338, 1995.

68 On Yao's XOR-Lemma

A fundamental lemma of Yao states that computational weak-unpredictability of functions gets amplified if the results of several independent instances are XOR-ed together. This work provides an exposition of three alternative proofs of Yao's Lemma, where the first one is due to Levin, the second one to Impagliazzo, and the third one is new.

Comments: Authored by O. Goldreich, N. Nisan and A. Wigderson. Appeared in

ECCC, TR95-050, 1995.

69 On Constructing 1-1 One-way Functions

It is shown how to construct length-preserving 1-1 one-way functions (rather than (infinite) families of (finite) one-way permutations) based on popular intractability assumptions (e.g., RSA, DLP).

Comments: Authored by O. Goldreich, L.A. Levin and N. Nisan. Appeared in

ECCC, TR95-029, 1995.

70 Incremental Cryptography and Application to Virus Protection

This work introduced Incremental Cryptography, where incrementality means that one can obtain the value of a cryptographic function on an input when given also the function's value on a related input, more efficiently than by applying the cryptographic function. In particular, it provides incremental signature and message authentication schemes supporting a variety of document modification operations.

Comments: Authored by M. Bellare, O. Goldreich and S. Goldwasser. Appeared in

- *Proc. of the 27th STOC*, pp. 45-56, 1995.

71 Private Information Retrieval

This work introduced Private Information Retrieval, which is a method to obtain information from a database that is split between several (non-colluding) servers without revealing any information about the specific record being retreived. The main result is a two-server scheme of communication complexity related to the third root of the length of the original database.

Comments: Authored by B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan. Appeared in

- *Proc. of the 36th FOCS*, pp. 41-50, 1995.
- *Jour. of the ACM*, Vol. 45, No. 6, pages 965–982, November 1998.

72 Free Bits, PCPs and Non-Approximability – Towards Tight Results

This 110-pages work contains numerous results regarding PCP and their relation to non-approximability results. In retrospect, the most influential contribution was the introduction of the Long-Code (and/or the demonstration of its usefulness for the design of PCPs).

Abstract (abbr.): This paper continues the investigation of the connection between probabilistically checkable proofs (PCPs) the approximability of NP-optimization problems. The emphasis is on proving tight non-approximability results via consideration of measures like the "free bit complexity" and the "amortized free bit complexity" of proof systems.
The first part of the paper presents a collection of new proof systems based on a new error-correcting code called the Long Code. We provide a proof system which has amortized free bit complexity arbitrary close to 2, implying that approximating Max-Clique (resp., the Chromatic Number) within a third root (resp., fifth root) of the number of vertices is NP-Hard under randomized reductions. We also derive the first explicit and reasonable constant hardness factors for Min Vertex Cover, Max-2SAT, and Max-Cut, and improve the hardness factor for Max-3SAT. We note a general approach to the derivation of strong non-approximability results under which the problem reduces to the construction of certain "gadgets."
The increasing strength of non-approximability results obtained via the PCP connection motivates us to ask how far this can go, and whether PCPs are inherent in any way. The second part of the paper addresses this. The main result is a "reversal" of the FGLSS connection: where the latter had shown how to translate proof systems for NP into NP-hardness of approximation results for Max-Clique, we show how any NP-hardness of approximation result for Max-Clique yields a proof system for NP. Roughly, our result says that for any constant f if Max-Clique is NP-hard to approximate within a *(f+1)*st root of the number of vertices then NP has a PCP of amortized free bit complexity f.
The third part of our paper initiates a systematic investigation of the properties of PCP and FPCP as a function of the various parameters: randomness, query complexity, free bit complexity, amortized free bit complexity, proof size, etc. We are particularly interested in "triviality" results, which indicate which classes are not powerful enough to capture NP. We also distill the role of randomized reductions in this area, and provide a variety of useful transformations between proof checking complexity classes.

Comments: Authored by M. Bellare, O. Goldreich and M. Sudan. Appeared in

- *Proc. of the 36th FOCS*, pp. 422-431, 1995.
- *SIAM Jour. on Comp.*, Vol. 27, No. 3, pp. 804–915, June 1998.

73 Learning polynomials with queries: the highly noisy case

This paper presents an algorithm for reconstructing all n-variant polynomials of degree d, over a finite field F, that agree with a given function on a given (small) fraction of the domain. Given oracle access to the function, the algorithm operates in time polynomailly related to n and the agreement parameter and exponential in d, provided that the agreement parameter is above some bound that refers to the ratio of the degree and the field size.

Comments: Authored by O. Goldreich, R. Rubinfeld and M. Sudan. Appeared in

- *Proc. of the 36th FOCS*, pp. 294-303, 1995.
- *SIAM J. on Disc. Math.*, Vol. 13, No. 4, pages 535–570, 2000.

74 Adaptively Secure Multi-party Computation

This work shows how to construct multi-party protocols that maintain their security with respect to adversaries that may adaptively corrupt a fraction of the parties during the course of the computation.

Comments: Authored by R. Canetti, U. Feige, O. Goldreich and M. Naor. Appeared in

- *Proc. of the 28th STOC*, pp. 639-648, 1996.

Sabbatical at MIT (1996–1998)

75 Property Testing and its connection to Learning and Approximation

This paper initiates a general treatment of Property Testing, while focusing on testing of graph properties in the adjacency matrix representation. The main results are testers for a variety of graph partition problems all having query complexity that is independent of the size of the graph (but rather depends only on the approximation parameter).

Abstract (rev.): We consider the question of determining whether a function f has a predetermined property P or is far from any function with property P. A property testing algorithm is given a sample of the value of f on instances drawn according to some distribution, and, in some cases, it is also allowed to query f on instances of its choice.
We establish some connections between property testing and problems in learning theory. Next, we focus our attention on testing graph properties, and devise algorithms to test whether a graph has properties such as being k-Colorable or having a rho-Clique (i.e., a clique of density rho). Our graph property testing algorithms are probabilistic and make assertions that are correct with high probability, utilizing a number of edge-queries (into the graph) that only depend (polynomially) on the distance parameter. Moreover, the property testing algorithms can be used to efficiently (i.e., in time linear in the number of vertices) to construct partitions of the graph that correspond to close approximations to the property being tested, if it holds for the input graph.

Comments: Authored by O. Goldreich, S. Goldwasser and D. Ron. Appeared in

- *Proc. of the 37th FOCS*, pp. 339–348, 1996.
- *Jour. of the ACM*, pages 653–750, July 1998.

76 On the Complexity of Interactive Proofs with Bounded Communication

This paper establishes a separation between interactive proofs and arguments, by showing that interactive proofs are unlikely to be as efficient as arguments. The paper contains results regarding various restrictions on the interactive proofs.

Comments: Authored by O. Goldreich and J. Hastad. Appeared in

- *IPL*, Vol. 67 (4), pages 205–214, 1998.

77 On the Circuit Complexity of Perfect Hashing

Comments: Authored by O. Goldreich and A. Wigderson. (It turns out that these results were known.) Appeared in

ECCC, TR96-041, 1996.

78 On Universal Learning Algorithms

It is shown that there exists a universal learning algorithm that PAC-learns every concept class within complexity that is linearly related to the complexity of the best learning algorithm for this class. This

observation is derived by an adaptation, to the learning context, of Levin's proof of the existence of optimal algorithms for NP.

Comments: Authored by O. Goldreich and D. Ron. Appeared in

- *IPL*, Vol. 63, 1997, pages 131–136.

79 Collision-Free Hashing from Lattice Problems

This work provides a survey of Ajtai's construction of one-way functions based on the assumption that certain approximation problems in lattices are difficuly in the worst-case. It is also shown that essentially the same construction can be used to obtain collision-free hashing.

Comments: Authored by O. Goldreich, S. Goldwasser and S. Halevi. Appeared in

ECCC, TR95-042, 1996.

80 Property Testing in Bounded Degree Graphs

This work initiates the study of testing graph properties in the bounded-length incidence lists model. In particular, it presence testing algorithms for connectivity and k-connectivity, and lower bounds on the query complexity of testing bipartiteness and graph expansion.

Comments: Authored by O. Goldreich and D. Ron. Appeared in

- *Proc. of the 29th STOC*, pages 406–415, 1997.
- *Algorithmica*, Vol. 32 (2), pages 302–343, 2002.

81 The Graph Clustering Problem has a Perfect Zero-Knowledge Proof

Comments: Authored by O. Goldreich. Appeared in

ECCC, TR96-054, November 1996.

- Journal version with A. De-Santis, G. Di-Crescenzo and G. Persiano, *IPL*, Vol. 69, pp. 201–206, 1999.

82 Public-Key Cryptosystems from Lattice Reduction Problems

This paper oresents a proposal for a trapdoor one-way function that is based on a computational problem regarding integer lattices.

Comments: Authored by O. Goldreich, S. Goldwasser and S. Halevi. (The security of the proposal is not rigorously related to any known conjecture. For the suggested security parameters, the proposal was broken a couple of years after its presentation.) Appeared in

- Proceedings of *Crypto97*, Springer LNCS, Vol. 1294, pp. 112–131.

83 Computational Indistinguishability – Algorithms vs. Circuits

It is shown that there exist pairs of distributions that are computationally indistinguishable by any probabilistic algorithms but are easily distinguishable by circuits. Furthermore, one distribution may be the uniform over strings of certain length, whereas the other may have a tiny support (of size that is any unbounded function of the string length).

Comments: Authored by O. Goldreich and B. Meyer. Appeared in

- *Theoretical Computer Science*, Vol. 191 (1998), pages 215–218.

84 Computational Sample Complexity

This work proves that there exist concept classes that (under similar cryptographic assumptions) possess arbitrary sized gaps between their standard (information-theoretic) sample complexity and their computational sample complexity (i.e., the size of the sample required by probabilistic polynomial-time learning algorithms). The same holds also with respect to learning from membership queries and learning from noisy examples.

Comments: Authored by S. Decatur, O. Goldreich and D. Ron. Appeared in

- *10th COLT*, pp. 130-142, 1997.
- *SIAM Jour. on Comp.*, Vol. 29, Nr. 3, pages 854–879, 1999.

85 Self-Delegation with Controlled Propagation – or – What If You Lose Your Laptop

Comments: Authored by O. Goldreich, B. Pfitzmann and R.L. Rivest. Appeared in

- Proceedings of *Crypto98*, Springer LNCS, Vol. 1462, pages 153–168.

86 Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem

Comments: Authored by O. Goldreich, S. Goldwasser and S. Halevi. Appeared in

- Proceedings of *Crypto97*, Springer LNCS, Vol. 1294, pp. 105–111.

87 Uniform Generation of NP-witnesses using an NP-oracle

This work presents a probabilistic polynomial-time oracle machine for uniformly generating instances in an NP-complete set when given oracle access to the set. The algorithm utilizes ideas originating in the works of Sipser, Stockmeyer, and Jerrum, Valiant and Vazirani, but the presentation is simpler and yields a stronger result.

Comments: Authored by M. Bellare, O. Goldreich and E. Petrank. Appeared in

- *Inform. and Comp.*, Vol. 163, pages 510–526, 2000.

88 Another proof that BPP subseteq PH (and more)

This work provides another proof of the Sipser–Lautemann Theorem by which BPP is contained in MA (which in turn is in PH). The current proof is based on known results regarding the amplification of BPP (or "error reduction"). Given these strong results, the current proof is even simpler than previous ones.

Comments: Authored by O. Goldreich and D. Zuckerman. Appeared in

ECCC, TR97-045, 1997.

89 Computational Indistinguishability: A Sample Hierarchy

This paper establishes the existence of pairs of distributions that can be efficiently distinguished given $k+1$ samples but cannot be distinguished given k samples, where in both cases we refer to uniform algorithms.

Comments: Authored by O. Goldreich and M. Sudan. Appeared in

- *Proc. of the 13th CCC*, pages 24-33, 1998.
- *JCSS*, Vol. 59, pages 253–269, 1999.

90 On the Limits of Non-Approximability of Lattice Problems

The work presents constant-round interactive proofs for two promise problems that capture approximation problems in lattices. Specifically, this refers to the Shortest Vector and Closest Vector problems, and the approximation factor is smaller than the square root of the dimention of the lattice.

Comments: Authored by O. Goldreich and S. Goldwasser. Appeared in

- *Proc. of the 30th STOC*, pp. 1–9, 1998.
- *JCSS*, Vol. 60, pages 540–563, 2000.

91 A Sublinear Bipartitness Tester for Bounded Degree Graphs

This work presents an almost optimal tester for bipartiteness in the bounded-length incidence lists model. The tester works by uniformly selecting a few start vertices, and taking many random walks on the graph from each start vertex, where the number of walks is approximately the square root of the number of vertices in the graph, and each walk has poly-logarithmic length. The tester accepts if and only if the subgraph seen by these walks is bipartite.

Comments: Authored by O. Goldreich and D. Ron. Appeared in

- *Proc. of the 30th STOC*, pp. 289–298, 1998.
- *Combinatorica*, Vol. 19 (3), pages 335–373, 1999.

92 The Random Oracle Methodology, Revisited

This work takes a critical look at the relationship between the security of cryptographic schemes in the Random Oracle Model, and the security of the schemes that result from implementing the random oracle by so called "cryptographic hash functions". It is shown that, in general, no such relation exist. Specifically, there exist signature and encryption schemes that are secure in the Random Oracle Model, but for which any implementation of the random oracle results in insecure schemes. This refutes the common belief that a security proof in the Random Oracle Model means that there are no "structural flaws" in the scheme, and that there can be no "generic attacks" against it.

Comments: Authored by R. Canetti, O. Goldreich and S. Halevi. Appeared in

- *Proc. of the 30th STOC*, pp. 209–218, 1998.

93 Honest-Verifier Statistical Zero-Knowledge Equals General Statistical Zero-Knowledge

This work provides a transformation of public-coin protocols that are zero-knowledge with respect to the honest verifier into protocols that are zero-knowledge in the general sense. The core of the transformation is an improved random selection protocol, which posses a strong simultability property.

Comments: Authored by O. Goldreich, A. Sahai and S. Vadhan. Appeared in

- *Proc. of the 30th ACM Symp. on Theory of Computing (STOC)*, pp. 399–408, 1998.

94 Testing Monotinicity

This work presents a (randomized) test for monotonicity of Boolean functions (i.e., mapping n-bit strings to a single bit). By querying the function at arguments of its choice, the test always accepts a monotone function, and rejects with high probability any function that is far from being monotone. The query complexity of the test is linear in n and in the inverse of the distance parameter.

Comments: Authored by O. Goldreich, S. Goldwasser, E. Lehman and D. Ron. Appeared in

- *Proc. of the 39th FOCS*, pages 426–435, 1998.
- Journal version with A. Samorodnitsky, *Combinatorica*, Vol. 20 (3), pages 301–337, 2000.

95 Deterministic Amplification of Space Bounded Probabilistic Algorithms

Comments: Authored by Z. Bar-Yossef, O. Goldreich and A. Wigderson. Appeared in

- Proceedings of *14th CCC*, pages 188–198, 1999.

96 Can Statistical Zero-Knowledge be Made Non-Interactive? or On the Relationship of SZK and NISZK

This work studies the class of sets having Non-Interactive Statistical Zero-Knowledge proofs. One of the results is that this class extends beyond BPP if and only if the corresponding interactive class (i.e., Statistical Zero-Knowledge) extends beyond BPP.

Comments: Authored by O. Goldreich, A. Sahai and S. Vadhan. Appeared in

- Proceedings of *Crypto99*, Springer LNCS, Vol. 1666, pages 467–484.

97 Comparing Entropies in Statistical Zero-Knowledge with Applications to the Structure of SZK

This work presents a public-coin Statistical Zero-Knowledge (SZK) proof for a promise problem regarding comparing the entropies of two given distributions. This protocol is used in order to provide a simpler proof of the fact that public-coin SZK equals general SZK.

Comments: Authored by O. Goldreich and S. Vadhan. Appeared in

- Proceedings of *14th CCC*, pages 54–73, 1999.

98 Beyond the Birthday Barrier, Without Counters

This work shows how to obtain approximately N (rather than square root of N) random values by using a random function defined on a domain of size N.

Comments: Authored by M. Bellare, O. Goldreich and H. Krawczyk. Appeared in

- Proceedings of *Crypto99*, Springer LNCS, Vol. 1666, pages 270–287.

99 Chinese Remaindering with Errors

This work presents algorithms for unique decoding and list decoding for an error correcting code based on the Chinese Remainder Theorem.

Comments: Authored by O. Goldreich, D. Ron and M. Sudan. Appeared in

- *Proc. of the 31st STOC*, pages 225–234, 1999.
- *IEEE Transactions on Information Theory*, Vol. 46, No. 4, July 2000, pages 1330–1338.

Back at Weizmann (1998 and onwards)

100 Approximating shortest lattice vectors is not harder than approximating closest lattice vectors

This work presents a Cook-reduction of the problem of approximating the shortest vector in a lattice to the problem of approximating the closest vectors in a lattice. The reduction is simple, preserves the level of approximation as well as the dimension of the lattice, and works both for the search and decision versions.

Comments: Authored by O. Goldreich, D. Micciancio, S. Safra and J.P. Seifert. Appeared in

- *IPL*, 71, pages 55–61, 1999.

101 Improved Testing Algorithms for Monotonicity

This work focuses on functions from the the n-wise Cartesian product of any ordered set to the reals, and presents a testing algorithm with complexity that is linear in n and polylogarithmic in the size of the basic set.

Comments: Authored by Y. Dodis, O. Goldreich, E. Lehman, S. Raskhodnikova, D. Ron and A. Samorodnitsky. Appeared in

- *Random99*, Springer LNCS, Vol. 1671, pages 97–108.

102 Improved Derandomization of BPP using a Hitting Set Generator

Comments: Authored by O. Goldreich and A. Wigderson. Appeared in

- *Random99*, Springer LNCS, Vol. 1671, pages 131–137.

103 Interleaved Zero-Knowledge in the Public-Key Model

Comments: Authored by O. Goldreich, S. Goldwasser and S. Micali. (This is a preliminary version of the next work.) Appeared in

ECCC, TR99-024, 1999.

104 Resettable Zero-Knowledge

This work introduces the notion of Resettable Zero-Knowledge (RZK), which means that the protocol remains zero-knowledge even if an adversary can interact with the prover many times, each time resetting the prover to its initial state and forcing it to use the same random tape. One of the results is a RZK proof system for NP.

Comments: Authored by R. Canetti, O. Goldreich, S. Goldwasser and S. Micali. Appeared in

- *Proc. of the 32nd STOC*, pages 235–244, 2000.

105 Simplified Derandomization of BPP using a Hitting Set Generator

Comments: Authored by O. Goldreich, S. Vadhan and A. Wigderson. Appeared in

ECCC, TR00-004, 2000.

106 On Pseudorandomness with respect to Deterministic Observers

This work provides an explanation to the fact that, in the (uniform-complexity) theory of pseudorandomness, potential (uniform) observers are modeled as probabilistic (rather than deterministic) polynomial-time machines.

Comments: Authored by O. Goldreich and A. Wigderson. Appeared in

- *Random00, ICALP workshops 2000*, Carleton Scientific (Proc. in Inform. 8), pages 77–84.

107 On Testing Expansion in Bounded-Degree Graphs

This work shows that a natural sub-linear time algorithm is a tester of graph expansion, provided that a plausible combinatorial conjecture holds.

Comments: Authored by O. Goldreich and D. Ron. Appeared in

ECCC, TR00-020, 2000.

108 Session-Key Generation using Human Passwords Only

This work presents session-key generation protocols in a model where the legitimate parties share only a human-memorizable password. The security guarantee holds with respect to probabilistic polynomial-time adversaries that control the communication channel (between the parties), and may omit, insert and modify messages at their choice. Loosely speaking, the effect of such an adversary that attacks an execution of the protocol is comparable to an attack in which an adversary is only allowed to make a constant number of queries of the form "is w the password of Party A".

Comments: Authored by O. Goldreich and Y. Lindell. Appeared in

- Proceedings of *Crypto01*, pages 408–432.

109 Candidate One-Way Functions Based on Expander Graphs

This work suggests a candidate one-way function using combinatorial constructs such as expander graphs. These graphs are used to determine a sequence of small overlapping subsets of input bits, to which a hard-wired random predicate is applied. The conjectured difficulty of inverting the suggested function does not seem to follow from any well-known assumption, but is rather proposed as an open problem,

Comments: Authored by O. Goldreich. Appeared in

Cryptology ePrint Archive, Report 2000/063, 2000.

ECCC, TR00-090, 2000.

110 On the Security of Modular Exponentiation with Application to the Construction of Pseudorandom Generators

O. Goldreich and V. Rosen,

Cryptology ePrint Archive, Report 2000/064, 2000.

111 On the (Im)possibility of Software Obfuscation

Informally, an *obfuscator* is an (efficient, probabilistic) "compiler" that takes as input a program P and produces a new program *Obf(P)* that has the same functionality as P yet is "unintelligible" in some sense. The main result of this work is that, even under very weak formalizations of the above notion, obfuscation is impossible.

Comments: Authored by B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang. Appeared in

- Proceedings of *Crypto01*, pages 1–18.

112 Three Theorems regarding Testing Graph Properties

This work presents three theorems regarding testing graph properties in the adjacency matrix representation. These theorems relate to the project of characterizing graph properties according to the complexity of testing them (in the adjacency matrix representation).

Comments: Authored by O. Goldreich and L. Trevisan. Appeared in

- Proceedings of *42nd FOCS*, pages 460–469, 2001.

113 On interactive proofs with a laconic provers

This work provides evidence that NP-complete sets cannot have interactive provers that are much more "laconic" (i.e., send significantly less bits) than the standard NP-proof. Specifically, the main result in this work shows that if L has an interactive proof in which the prover sends b bits to the verifier, then the complement of L has a *constant-round* interactive proof of complexity that depends only exponentially on b.

Comments: Authored by O. Goldreich, S. Vadhan and A. Wigderson. Appeared in

- Proceedings of *28th ICALP*, Springer's LNCS 2076, pages 334–345, 2001.

114 Resettably-Sound Zero-Knowledge and its Applications

This work introduces resettably-sound proofs and arguments, which are protocols that maintain their soundness even when the prover can reset the verifier to use the same random coins in repeated executions of the protocol. It shows that resettably-sound zero-knowledge arguments for NP exist if collision-free hashing functions exist, whereas resettably-sound zero-knowledge proofs are possible only for languages in P/poly.

Comments: Authored by B. Barak, O. Goldreich, S. Goldwasser and Y. Lindell. Appeared in

- Proceedings of *42nd FOCS*, pages 116–125, 2001.

115 Lower Bounds for Linear Locally Decodable Codes and Private Information Retrieval

The main result of this work is an exponential lower-bound on the length of linear codes that allow to recover each desired information bit by probing the corrupted codeword at two (random) positions.

Comments: Authored by O. Goldreich, H. Karloff, L. Schulman and L. Trevisan. Appeared in

- Proceedings of *17th CCC*, pages 175–183, 2002.

116 Concurrent Zero-Knowledge With Timing, Revisited

This work shows that a known constant-round zero-knowledge proof for NP preserves its security when polynomially-many independent copies are executed concurrently under the above timing model. The analysis combines the treatment of two extreme schedulings of concurrent executions under the above timing model: the first extreme scheduling, which is of independent interest, is the *parallel execution* of polynomially-many copies.

Comments: Authored by O. Goldreich. Appeared in

- *Proc. of the 34th STOC*, pages 332–340, 2002.

117 Universal arguments and their applications

Universal-arguments are computationally-sound proof systems that combine instance-based prover-efficiency condition of CS-proofs with the computational-soundness condition of argument systems. This work shows that universal-arguments can be constructed based on standard intractability assumptions that refer to polynomial-size circuits (rather than assumptions referring to subexponential-size circuits as used in the construction of CS-proofs), and that the former suffice for Barak's non-black-box zero-knowledge arguments.

Comments: Authored by B. Barak and O. Goldreich. Appeared in

- Proceedings of *17th CCC*, pages 194–203, 2002.

118 Using the FGLSS-reduction to Prove Inapproximability Results for Minimum Vertex Cover in Hypergraphs

This work demonstrates the applicability of the FGLSS-reduction in the context of reductions among combinatorial optimization problems.

Comments: Authored by O. Goldreich. Appeared in

ECCC, TR01-102, 2001.

119 On Chosen Ciphertext Security of Multiple Encryptions

This work shows that the standrad technical definition of Chosen Ciphertext Security implies a natural definition that is formulated in terms of semantic security and refers to "multiple-target" attacks.

Comments: Authored by O. Goldreich, Y. Lustig and M. Naor. Appeared in

120 Locally Testable Codes and PCPs of Almost-Linear Length

Locally testable codes are error-correcting codes that admit very efficient codeword tests (i.e., involving a constant number of queries). This work presents locally testable codes and PCPs of almost-linear length, where almost-linear means smaller than any constant power that is greater than 1.

Comments: Authored by O. Goldreich and M. Sudan. Appeared in

121 Deradomization that is rarely wrong from short advice that is typically good

One result presented in this work is a log-space deterministic algorithm that correctly decides undirected connectivity on all but a sub-exponential number of graphs of a certain size. This and other results are

obtained as special cases of a general methodology that evolves around short (and typically-good) advice strings.

Comments: Authored by O. Goldreich and A. Wigderson. Appeared in