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.


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

Graduate School (1981–83) 1
1 The Minimum Length Generator Sequence is NP-Hard 1
2 DES-Like Functions Can Generate the Alternating Group 1
3 On the NP-Completeness of Certain Network-Testing Problems 1
4 A Randomized Protocol for Signing Contracts 1
5 On The Security of Multi-Party Ping-Pong Protocols 1
6 A Simple Protocol for Signing Contracts 2
7 Electronic Wallet 2
8 On the Power of Cascade Ciphers 2
9 On Concurrent Identification Protocols 2

The Post-Doctoral Period (1983–86) 3
10 How to Construct Random Functions 3
11 Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle is NP-Hard 3
12 The Weakest Pseudo-Random Generator Implies the Strongest One 3
13 On the Number of Monochromatic and Close Beads in a Rosary 3
14 RSA/Rabin Functions: Certain Parts are As Hard As the Whole 4
15 On the Cryptographic Applications of Random Functions 4
16 On the Power of Two–Point Based Sampling 5
17 Global Computation in the Presence of Link Failures – The Case of a Ring 5
18 Electing a Leader in a Ring with Link Failures 5
19 Unbiased Bits From Sources of Weak Randomness 5
20 The Bit Extraction Problem or t-Resilient Functions 6
21 An Improved Parallel Algorithm for Integer GCD 6
22 A Fair Protocol for Signing Contracts 6
23 On the Security of Ping-Pong Protocols when Implemented Using the RSA 7
24 The Bit Security of Modular Squaring given Partial Factorization of the Modulus 7
25 Two Remarks Concerning the GMR Signature Scheme 7
26 All Languages in NP have Zero-Knowledge Proofs 7
27 Towards a Theory of Software Protection and Simulation by Oblivious RAMs 8
28 A Completeness Theorem for Protocols with Honest Majority 8
29 Everything Provable is Provable in Zero-Knowledge 8

The Technion Period (1986–94) 9
30 On the Time-Complexity of Broadcast in Radio Networks 9
31 Efficient Emulation of Single-Hop Radio Network with Collision Detection
32 How to Solve any Protocol Problem – An Efficiency Improvement
33 On Completeness and Soundness in Interactive Proof Systems
34 A Trade-off between Information and Communication in Broadcast Protocols
35 Definitions and Properties of Zero-Knowledge Proof Systems
36 On the Existence of Pseudorandom Generators
37 A Perfect Zero-Knowledge Proof for a Problem Equivalent to Discrete Logarithm
38 On-line/Off-line Digital signatures
39 Hard-core Predicates for any One-Way Function
40 On the Theory of Average Case Complexity
41 Guaranteeing Termination in Fast Randomized Byzantine Agreement Protocols
42 On the Composition of Zero-Knowledge Proof Systems
43 A Note on Computational Indistinguishability
44 Quantifying Knowledge Complexity
45 On Sparse Pseudorandom Ensembles
46 How to Construct Constant-Round Zero-Knowledge Proof Systems for NP
47 Source to Destination Communication in the Presence of Faults
48 A Uniform Complexity Treatment of Encryption and Zero-Knowledge
49 A Quantitative Approach to Dynamic Networks
50 Security Preserving Amplification of Hardness
51 Simple Constructions of Almost k-wise Independent Random Variables
52 Bounds on Tradeoffs between Randomness and Communication Complexity
53 Randomness in Interactive Proofs
54 The Random Oracle Hypothesis is False
55 Fault-tolerant Computations without Assumptions: the Two-party Case
56 Approximations of General Independent Distributions
57 Towards a Computational Theory of Statistical Tests
58 Global Computation in the Presence of Link Failures: the case of Unidirectional Faults
59 On Defining Proofs of Knowledge
60 Proofs of Computational Ability
61 Asynchronous Secure Computation
62 Lower Bounds for Sampling Algorithms for Estimating the Average
63 Tiny Families of Functions with Random Properties
64 Knowledge Complexity and Computational Complexity

The First 1.5 Years at Weizmann (1994–96)
<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>65</td>
<td>Incremental Cryptography: the Case of Hashing and Signing</td>
</tr>
<tr>
<td>66</td>
<td>A Combinatorial Consistency Lemma with application to the PCP Theorem</td>
</tr>
<tr>
<td>67</td>
<td>Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs</td>
</tr>
<tr>
<td>68</td>
<td>On Yao’s XOR-Lemma</td>
</tr>
<tr>
<td>69</td>
<td>On Constructing 1-1 One-way Functions</td>
</tr>
<tr>
<td>70</td>
<td>Incremental Cryptography and Application to Virus Protection</td>
</tr>
<tr>
<td>71</td>
<td>Private Information Retrieval</td>
</tr>
<tr>
<td>72</td>
<td>Free Bits, PCPs and Non-Approximability – Towards Tight Results</td>
</tr>
<tr>
<td>73</td>
<td>Learning polynomials with queries: the highly noisy case</td>
</tr>
<tr>
<td>74</td>
<td>Adaptively Secure Multi-party Computation</td>
</tr>
<tr>
<td>76</td>
<td>Property Testing and its connection to Learning and Approximation</td>
</tr>
<tr>
<td>77</td>
<td>On the Complexity of Interactive Proofs with Bounded Communication</td>
</tr>
<tr>
<td>78</td>
<td>On the Circuit Complexity of Perfect Hashing</td>
</tr>
<tr>
<td>79</td>
<td>On Universal Learning Algorithms</td>
</tr>
<tr>
<td>80</td>
<td>Collision-Free Hashing from Lattice Problems</td>
</tr>
<tr>
<td>81</td>
<td>Property Testing in Bounded Degree Graphs</td>
</tr>
<tr>
<td>82</td>
<td>The Graph Clustering Problem has a Perfect Zero-Knowledge Proof</td>
</tr>
<tr>
<td>83</td>
<td>Computational Indistinguishability – Algorithms vs. Circuits</td>
</tr>
<tr>
<td>84</td>
<td>Computational Sample Complexity</td>
</tr>
<tr>
<td>85</td>
<td>A Probabilistic Error-Correcting Scheme that Provides Partial Secrecy</td>
</tr>
<tr>
<td>86</td>
<td>Self-Delegation with Controlled Propagation – or – What If You Lose Your Laptop</td>
</tr>
<tr>
<td>87</td>
<td>Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem</td>
</tr>
<tr>
<td>88</td>
<td>Uniform Generation of NP-witnesses using an NP-oracle</td>
</tr>
<tr>
<td>89</td>
<td>Another proof that BPP subseteq PH (and more)</td>
</tr>
<tr>
<td>90</td>
<td>Computational Indistinguishability: A Sample Hierarchy</td>
</tr>
<tr>
<td>91</td>
<td>On the Limits of Non-Approximability of Lattice Problems</td>
</tr>
<tr>
<td>92</td>
<td>A Sublinear Bipartitness Tester for Bounded Degree Graphs</td>
</tr>
<tr>
<td>93</td>
<td>The Random Oracle Methodology, Revisited</td>
</tr>
<tr>
<td>94</td>
<td>Honest-Verifier Statistical Zero-Knowledge Equals General Statistical Zero-Knowledge</td>
</tr>
<tr>
<td>95</td>
<td>Testing Monotinicity</td>
</tr>
<tr>
<td>96</td>
<td>Deterministic Amplification of Space Bounded Probabilistic Algorithms</td>
</tr>
<tr>
<td>97</td>
<td>On the Relationship of SZK and NISZK</td>
</tr>
<tr>
<td>98</td>
<td>Comparing Entropies in Statistical Zero-Knowledge with Applications</td>
</tr>
</tbody>
</table>

101 Approximating shortest lattice vectors is not harder than approx. closest lattice vectors
102 Improved Testing Algorithms for Monotonicity
103 Improved Derandomization of BPP using a Hitting Set Generator
104 Interleaved Zero-Knowledge in the Public-Key Model
105 Resettable Zero-Knowledge
106 Simplified Derandomization of BPP using a Hitting Set Generator
107 On Pseudorandomness with respect to Deterministic Observers
108 On Testing Expansion in Bounded-Degree Graphs
109 Session-Key Generation using Human Passwords Only
110 Candidate One-Way Functions Based on Expander Graphs
111 On the Security of Modular Exponentiation
112 On the (Im)possibility of Software Obfuscation
113 Three Theorems regarding Testing Graph Properties
114 On interactive proofs with a laconic provers
115 Resettably-Sound Zero-Knowledge and its Applications
116 Lower Bounds for Linear Locally Decodable Codes and Private Information Retrieval
117 Concurrent Zero-Knowledge With Timing, Revisited
118 Universal arguments and their applications
119 Using the FGLSS-reduction to Prove Inapproximability Results
120 On Chosen Ciphertext Security of Multiple Encryptions
121 Locally Testable Codes and PCPs of Almost-Linear Length
122 Derandomization that is rarely wrong from short advice that is typically good
123 Almost k-wise independence versus k-wise independence
124 The GGM Construction does NOT yield Correlation Intractable Function Ensembles
125 Bounds on 2-Query Codeword Testing
126 On the Implementation of Huge Random Objects
127 On the random-oracle methodology as applied to length-restricted signature schemes


128 Robust PCPs of Proximity, Shorter PCPs and Applications to Coding
129 On Estimating the Average Degree of a Graph
130 From logarithmic advice to single-bit advice
<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>131</td>
<td>The Power of Verification Queries in Message Authentication and Authenticated Encryption</td>
<td>33</td>
</tr>
<tr>
<td>132</td>
<td>Short PCPs Verifiable in Polylogarithmic Time</td>
<td>33</td>
</tr>
<tr>
<td>133</td>
<td>Approximating Average Parameters of Graphs</td>
<td>33</td>
</tr>
<tr>
<td>134</td>
<td>On Basing One-Way Functions on NP-Hardness</td>
<td>34</td>
</tr>
<tr>
<td>135</td>
<td>On Expected Probabilistic Polynomial-Time Adversaries</td>
<td>34</td>
</tr>
<tr>
<td>136</td>
<td>On Probabilistic versus Deterministic Provers in the Definition of Proofs Of Knowledge</td>
<td>34</td>
</tr>
<tr>
<td>137</td>
<td>On the randomness complexity of property testing</td>
<td>34</td>
</tr>
<tr>
<td>138</td>
<td>On approximating the average distance between points</td>
<td>34</td>
</tr>
<tr>
<td>139</td>
<td>On the Average-Case Complexity of Property Testing</td>
<td>35</td>
</tr>
<tr>
<td>140</td>
<td>The Tensor Product of Two Good Codes Is Not Necessarily Robustly Testable</td>
<td>35</td>
</tr>
<tr>
<td>141</td>
<td>A Small Gap in the Gap Amplification of Assignment Testers</td>
<td>35</td>
</tr>
<tr>
<td>142</td>
<td>Algorithmic Aspects of Property Testing in the Dense Graphs Model</td>
<td>35</td>
</tr>
<tr>
<td>143</td>
<td>On Proximity Oblivious Testing</td>
<td>35</td>
</tr>
<tr>
<td>144</td>
<td>Hierarchy Theorems for Property Testing</td>
<td>36</td>
</tr>
<tr>
<td>145</td>
<td>From absolute distinguishability to positive distinguishability</td>
<td>36</td>
</tr>
<tr>
<td>146</td>
<td>A Candidate Counterexample to the Easy Cylinders Conjecture</td>
<td>36</td>
</tr>
<tr>
<td>147</td>
<td>A Theory of Goal-Oriented Communication</td>
<td>36</td>
</tr>
<tr>
<td>148</td>
<td>More Constructions of Lossy and Correlation-Secure Trapdoor Functions</td>
<td>37</td>
</tr>
<tr>
<td>149</td>
<td>Testing Graph Blow-Up</td>
<td>37</td>
</tr>
<tr>
<td>150</td>
<td>Proximity Oblivious Testing and the Role of Invariances</td>
<td>37</td>
</tr>
<tr>
<td>151</td>
<td>Finding Cycles and Trees in Sublinear Time</td>
<td>37</td>
</tr>
<tr>
<td>152</td>
<td>On Testing Computability by Small Width OBDDs</td>
<td>37</td>
</tr>
<tr>
<td>153</td>
<td>In a World of P=BPP</td>
<td>38</td>
</tr>
<tr>
<td>154</td>
<td>Input-Oblivious Proof Systems and a Uniform Complexity Perspective on P/poly</td>
<td>38</td>
</tr>
<tr>
<td>155</td>
<td>Two Comments on Targeted Canonical Derandomizers</td>
<td>38</td>
</tr>
<tr>
<td>156</td>
<td>Enhancements of Trapdoor Permutations</td>
<td>38</td>
</tr>
<tr>
<td>157</td>
<td>Monotone Circuits: One-Way Functions versus Pseudorandom Generators</td>
<td>38</td>
</tr>
<tr>
<td>158</td>
<td>On the Effect of the Proximity Parameter on Property Testers</td>
<td>39</td>
</tr>
<tr>
<td>159</td>
<td>Two-Sided Error Proximity Oblivious Testing</td>
<td>39</td>
</tr>
<tr>
<td>160</td>
<td>On the possibilities and limitations of pseudodeterministic algorithms</td>
<td>39</td>
</tr>
<tr>
<td>161</td>
<td>On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions</td>
<td>39</td>
</tr>
</tbody>
</table>

**Sabbatical at IAS (2011–12)**

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>156</td>
<td>Enhancements of Trapdoor Permutations</td>
<td>38</td>
</tr>
<tr>
<td>157</td>
<td>Monotone Circuits: One-Way Functions versus Pseudorandom Generators</td>
<td>38</td>
</tr>
<tr>
<td>158</td>
<td>On the Effect of the Proximity Parameter on Property Testers</td>
<td>39</td>
</tr>
<tr>
<td>159</td>
<td>Two-Sided Error Proximity Oblivious Testing</td>
<td>39</td>
</tr>
<tr>
<td>160</td>
<td>On the possibilities and limitations of pseudodeterministic algorithms</td>
<td>39</td>
</tr>
</tbody>
</table>

**Back at Weizmann (2012–2019)**

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>161</td>
<td>On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions</td>
<td>39</td>
</tr>
</tbody>
</table>
196 One-Sided Error Testing of Monomials and Affine Subspaces

197 On Counting \( t \)-Clique Mod 2

198 On Testing Hamiltonicity in the Bounded Degree Graph Model

199 On Testing Asymmetry in the Bounded Degree Graph Model

200 Robustly Self-Ordered Graphs: Constructions and Applications to Property Testing

Back at Weizmann (2020–)

201 Non-adaptive vs Adaptive Queries in the Dense Graph Testing Model

202 Constructing Large Families of Pairwise Far Permutations: Good Permutation Codes Based on the Shuffle-Exchange Network
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.

Credits: Authored by S. Even and O. Goldreich.\(^1\) Appeared in

2 DES-Like Functions Can Generate the Alternating Group

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

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

Credits: Authored by S. Even, O. Goldreich, S. Moran and P. Tong.\(^2\) Appeared in

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 demonstrated, and so is its applicability.

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

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 attacks) and to restricted classes of protocols. The computational task of testing whether or not such protocols are insecure is studied, and is shown to be undecidable for one of the classes and NP-hard for another.

\(^1\)Indeed, this was my first paper.
\(^2\)This was my M.Sc. Thesis.
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 effect 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.

Credits: Authored by S. Even and O. Goldreich.\(^3\) Appeared in


6 A Simple Protocol for Signing Contracts

Credits: Authored by O. Goldreich. Appeared in


7 Electronic Wallet

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


8 On the Power of Cascade Ciphers

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


9 On Concurrent Identification Protocols

Credits: Authored by O. Goldreich. Appeared in


\(^3\)This was the main part of my D.Sc. Thesis.
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 pseudorandom 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 truly 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 arguments of its choice. The result has applications in cryptography, random coinstructions, and complexity theory.

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


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

Credits: Authored by O. Goldreich.


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 stretching functions.

Credits: 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.)

Credits: Authored by O. Goldreich. Appeared in


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 pseudorandom generators and probabilistic encryption schemes that are based on the intractability of factoring.

Credits: Authored by W. Alexi, B. Chor, O. Goldreich and C. P. Schnorr. Appeared in
- (partial result w/ B. Chor only), Crypto84 (Proceedings), Lecture Note in Computer Science (196) Springer Verlag, pp. 303–313, 1985.

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.

Credits: Authored by O. Goldreich, S. Goldwasser and S. Micali. Appeared in
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 guaranteed to intersect, with high probability, any set of non-negligible density.

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

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

Credits: Authored by O. Goldreich and L. Shiri. Appeared in

18 Electing a Leader in a Ring with Link Failures

Credits: Authored by O. Goldreich and L. Shiri. Appeared in

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).

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

- Proc. of the 26th FOCS, 1985, pp. 429-442.

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.

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


21 An Improved Parallel Algorithm for Integer GCD

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


22 A Fair Protocol for Signing Contracts

The contribution of this work is mostly non-technical: It reviews several possible interpretations of fairness and argues in favour of an information theoretic one.

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

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

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

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

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

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.

Credits: Authored by O. Goldreich. Appeared in

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.

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

Credits: Authored by O. Goldreich. Appeared in

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.

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

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.
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.

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


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

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


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.

Credits: 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.

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

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

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

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

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-triviality of zero-knowledge requires that both the prover and the verifier employ randomized strategies.

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

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.

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

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.

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

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.

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

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


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 accumulative function as considered by Levin).

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


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.

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

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.

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

43 A Note on Computational Indistinguishability

The non-triviality of the notion of computational indistinguishability, for sampleable distributions, is shown to be equivalent to the existence of pseudorandom generators. That is, it is shown how to transform two sampleable distributions that are computationally indistinguishable but statistically far apart, into a pseudorandom generator.

Credits: Authored by O. Goldreich. Appeared in

44 Quantifying Knowledge Complexity

This paper introduces several measures of the amount of knowledge gained via interaction, and investigates the relations among them. (In all cases, a zero amount of knowledge coincides with zero-knowledge.)

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

45 On Sparse Pseudorandom Ensembles

The existence of pseudorandom distributions of various types is proved. The focus is on “evasive” distributions (i.e., distributions for which it is infeasible to generate any element in their support).

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

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

The natural construction, in which the verifier first commits to queries, and then a query-response protocol takes place, is shown to work. One key ingredient in the proof is solving a technical problem that arises in the simulation of this construction.
47 Source to Destination Communication in the Presence of Faults

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

48 A Uniform Complexity Treatment of Encryption and Zero-Knowledge

This paper presents definitions that refer to the infeasibility 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.

Credits: Authored by O. Goldreich. Appeared in

49 A Quantitative Approach to Dynamic Networks

The core of this approach is in quantifying the reliability (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.

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

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 successive iterations with moves on an adequate expander graph.

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

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.

Credits: Authored by N. Alon, O. Goldreich, J. Hastad and R. Peralta. Appeared in
52  Bounds on Tradeoffs between Randomness and Communication Complexity

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

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.

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

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.

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

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

In retrospect, the most interesting 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.

Credits: Authored by O. Goldreich, S. Goldwasser and N. Linial. Appeared in
56 Approimations 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.

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

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.

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

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

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

59 On Defining Proofs of Knowledge

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

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

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.

Credits: Authored by M. Bellare and O. Goldreich. (Unpublished manuscript, 1992.) See also
- Theory of Cryptography Library, record Arc-03.
61 Asynchronous Secure Computation

This work extends the definitions and constructions of secure multi-party protocols from the synchronous case to the asynchronous one.

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


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.

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


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

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

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

- Proc. of the 26th STOC, pp. 574-583, 1994.

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-oracle.

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


The First 1.5 Years at Weizmann (1994–96)

65 Incremental Cryptography: the Case of Hashing and Signing

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

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.

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

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”).

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

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.

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

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).

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

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 pro-
vides incremental signature and message authentication schemes supporting a variety of document
modification operations.

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

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 retrieved. The main result is a two-server scheme of communication
complexity related to the third root of the length of the original database.

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

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.

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


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 polynomially 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.

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

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.

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


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.

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

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.

Credits: Authored by O. Goldreich and J. Hastad. Appeared in
On the Circuit Complexity of Perfect Hashing

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

- ECCC, TR96-041, 1996.

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.

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


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 difficult in the worst-case. It is also shown that essentially the same construction can be used to obtain collision-free hashing.

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

- ECCC, TR96-042, 1996.

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.

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


The Graph Clustering Problem has a Perfect Zero-Knowledge Proof

Credits: Authored by O. Goldreich. Appeared in

- ECCC, TR96-054, November 1996.

82 Public-Key Cryptosystems from Lattice Reduction Problems

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

Credits: 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

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).

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

84 Computational Sample Complexity

Using standard intractability assumptions, this work proves that there exist concept classes that 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.

Credits: Authored by S. Decatur, O. Goldreich and D. Ron. Appeared in
- 10th COLT, pp. 130-142, 1997.

85 A Probabilistic Error-Correcting Scheme that Provides Partial Secrecy

A technical tool developed in the previous work is an error-correcting encoding scheme for which relatively few bits in the codeword yield no information about the plain message.

Credits: Authored by S. Decatur, O. Goldreich and D. Ron.

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

Credits: Authored by O. Goldreich, B. Pfitzmann and R.L. Rivest. Appeared in
87 Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem

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

88 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.

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

89 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.

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

90 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.

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

91 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 dimension of the lattice.

Credits: Authored by O. Goldreich and S. Goldwasser. Appeared in
- Proc. of the 30th STOC, pp. 1–9, 1998.
92 A Sublinear Bipartiteness 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.

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

93 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.

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

94 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.

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

95 Testing Monotonicity

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.

Credits: Authored by O. Goldreich, S. Goldwasser, E. Lehman and D. Ron. Appeared in
96 Deterministic Amplification of Space Bounded Probabilistic Algorithms

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


97 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.

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


98 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.

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


99 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 $N$.

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


100 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.

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


101 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.

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

102 Improved Testing Algorithms for Monotonicity

This work focuses on functions from 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.

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

103 Improved Derandomization of BPP using a Hitting Set Generator

A hitting-set generator is an algorithm that generates a set of strings that hit any sufficiently dense set that is recognizable by a small circuit. Andreev, Clementi, Rolin and Trevisan showed that if polynomial-time hitting-set generators exist then BPP equals P. This work simplify and tighten their argument.

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

104 Interleaved Zero-Knowledge in the Public-Key Model

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

105 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.
106  Simplified Derandomization of BPP using a Hitting Set Generator

This work further simplifies the use of a hitting set generator in the derandomization of BPP.

Credits: Authored by O. Goldreich, S. Vadhan and A. Wigderson. Appeared in
- ECCC, TR00-004, 2000.

107  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.

Credits: Authored by O. Goldreich and A. Wigderson. Appeared in
- Random00, ICALP workshops 2000, Carleton Scientific (Proc. in Inform. 8), pages 77–84.

108  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.

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

109  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 \( A \)”.

Credits: Authored by O. Goldreich and Y. Lindell. Appeared in
- Proceedings of Crypto01, pages 408–432.

110  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.

Credits: Authored by O. Goldreich. Appeared in
- ECCC, TR00-090, 2000.

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

Building on the work of Hastad, Schrift and Shamir, this work presents a simplified proof to the simultaneous security of the top bits with respect to exponentiation modulo a composite number.

Credits: Authored by O. Goldreich and V. Rosen. Appeared in

112 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 \( \text{Obf}(P) \) 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.

Credits: 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.

113 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). Issues addressed include the existence of monotone graph properties that are hard to test, and canonical testers for graph properties.

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

114 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 \textit{constant-round} interactive proof of complexity that depends only exponentially on \( b \).

\textbf{Credits:} Authored by O. Goldreich, S. Vadhan and A. Wigderson. Appeared in


115 \textbf{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.

\textbf{Credits:} Authored by B. Barak, O. Goldreich, S. Goldwasser and Y. Lindell. Appeared in


116 \textbf{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.

\textbf{Credits:} Authored by O. Goldreich, H. Karloff, L. Schulman and L. Trevisan. Appeared in


117 \textbf{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 \textit{parallel execution} of polynomially-many copies.

\textbf{Credits:} Authored by O. Goldreich. Appeared in

- In \textit{Theoretical Computer Science: Essays in Memory of Shimon Even}, Festschrift series of Springer's LNCS (as Vol 3895), pages 27–87, March 2006.
118 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.

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


119 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.

Credits: Authored by O. Goldreich. Appeared in


120 On Chosen Ciphertext Security of Multiple Encryptions

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

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


121 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.

Abstract (abbr.): We initiate a systematic study of locally testable codes; that is, error-correcting codes that admit very efficient membership tests. Specifically, these are codes accompanied with tests that make a constant number of (random) queries into any given word and reject non-codewords with probability proportional to their distance from the code. Locally testable codes are believed to be the combinatorial core of PCPs. However, the relation is less immediate than commonly believed. Nevertheless, we show that certain PCP systems can be modified to yield locally testable codes. On the other hand, we adapt techniques that we develop for the construction of the latter to yield new PCPs. Our main results are locally testable codes and PCPs of almost-linear length.
122 Derandomization 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.

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

123 Almost k-wise independence versus k-wise independence

Considering distributions over \( n \)-bit long strings, this work relates two natural notions of being approximately \( k \)-wise independent. The local notion refers to the distances of the various projections on any \( k \) coordinates, whereas the global notion refers to the distance from a single \( k \)-wise independent distribution.

Credits: Authored by N. Alon, O. Goldreich and Y. Mansour. Appeared in

124 The GGM Construction does NOT yield Correlation Intractable Function Ensembles

The GGM construction is a natural way to obtain pseudorandom function ensembles from arbitrary pseudorandom generators. This work shows that, in general, this construction does not yield correlation intractable ensembles. Specifically, it may happen that, given a description of such a function, one can easily find an input that is mapped to zero under this function.

Credits: Authored by O. Goldreich. Appeared in

125 Bounds on 2-Query Codeword Testing

This work provides upper bounds on the size of codes that are locally testable by querying only two input symbols. These upper bounds are applicable to linear codes as well as to general binary codes having one-sided error testers.

Credits: Authored by E. Ben-Sasson, O. Goldreich and M. Sudan. Appeared in
126 On the Implementation of Huge Random Objects

This work initiates a general investigation of pseudo-random implementations of huge random objects, and apply it to areas in which random objects occur naturally. A pseudo-random implementation of such type T object must generate objects of type T (which can not be distinguished from random), rather than objects which can not be distinguished from random type T objects (although they are not type T at all).

Credits: Authored by O. Goldreich, S. Goldwasser and A. Nussboim. Appeared in

127 On the random-oracle methodology as applied to length-restricted signature schemes

In this work, we extend our negative result (regarding the random-oracle methodology) to address also length-restricted signature schemes.

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


128 Robust PCPs of Proximity, Shorter PCPs and Applications to Coding

Abstract (abbr.): We continue the study of the trade-off between the length of PCPs and their query complexity. In particular, we present PCPs of double-logarithmic query complexity while incurring only a quasi-polylogarithmic overhead (over the standard NP-proof) in the proof length.

Our techniques include the introduction of a new variant of PCPs that we call “Robust PCPs of Proximity”. These new PCPs facilitate proof composition, which is a central ingredient in construction of PCP systems. Our main technical contribution is a construction of a “length-efficient” Robust PCP of Proximity. While the new construction uses many of the standard techniques in PCPs, it does differ from previous constructions in fundamental ways, and in particular does not use the “parallelization” step of Arora et al. The alternative approach may be of independent interest.

We also obtain analogous quantitative results for locally testable codes. In addition, we introduce a relaxed notion of locally decodable codes, and present such codes of almost-linear length.

Credits: Authored by E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Appeared in

32
On Estimating the Average Degree of a Graph

Using “neighbor queries” as well as “degree queries”, we show that the average degree of a graph can be approximated arbitrarily well in sublinear time.

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

From logarithmic advice to single-bit advice

This work makes explicit a technique that translates time-separation results regarding short (say logarithmic) advice into separations for a single-bit advice.

Credits: Authored by O. Goldreich, M. Sudan and L. Trevisan. Appeared in

Back at Weizmann (2004–2011)

The Power of Verification Queries in Message Authentication and Authenticated Encryption

A popular belief is investigated, showing that its simple form is false and that an augmented version of it is valid.

Credits: Authored by M. Bellare, O. Goldreich and A. Mityagin. Appeared in

Short PCPs Verifiable in Polylogarithmic Time

This work shows that every language in NP has a probabilistically checkable proof of proximity (i.e., proofs asserting that an instance is “close” to a member of the language), where the verifier’s running time is polylogarithmic in the input size and the length of the probabilistically checkable proof is only polylogarithmically larger that the length of the classical proof.

Credits: Authored by E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. Vadhan. Appeared in

Approximating Average Parameters of Graphs

This work initiates a study of sublinear randomized algorithms for approximating average parameters of a graph. Specifically, it refers to the average degree of a graph and the average distance between pairs of vertices in a graph, and indicates a difference between the two problems.

Credits: Authored by O. Goldreich and D. Ron. Appeared in
134 On Basing One-Way Functions on NP-Hardness

This work examines the possibility of reductions from a worst-case decision problem to the task of average-case inverting a polynomial-time computable function $f$. (i.e., reductions that are supposed to establish that $f$ is one-way based on a worst-case assumption regarding the decision problem). The results illustrate the gain of directly studying the context of one-way functions rather than inferring results for this context from a the general study of worst-case to average-case reductions.

Credits: Authored by A. Akavia, O. Goldreich, S. Goldwasser and D. Moshkovitz. Appeared in

135 On Expected Probabilistic Polynomial-Time Adversaries: A suggestion for restricted definitions and their benefits

This work suggests restricted definitions of expected probabilistic polynomial-time adversaries, advocates their conceptual adequacy, and points out their technical advantages.

Credits: Authored by O. Goldreich. Appeared in

136 On Probabilistic versus Deterministic Provers in the Definition of Proofs Of Knowledge

This work points out a gap between two natural formulations of the concept of a proof of knowledge, and shows that in all natural cases (e.g., NP-statements) this gap can be closed.

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

137 On the randomness complexity of property testing

This work initiates a general study of the randomness complexity of property testing, aimed at reducing the randomness complexity of testers without (significantly) increasing their query complexity. It presents both generic existential bounds and efficient algorithms in specific cases.

Credits: Authored by O. Goldreich and O. Sheffet. Appeared in

138 On approximating the average distance between points

This work studies two algorithmic approaches to the problem of approximating the average distance between pairs of points in a high-dimensional Euclidean space, and more generally in any metric space.

Credits: Authored by K. Barhum, O. Goldreich and A. Shraibman. Appeared in
139  On the Average-Case Complexity of Property Testing

Considering the average-case complexity of property testing, this work points out that with respect to the uniform distribution property testing is trivial.

Credits: Authored by O. Goldreich. Appeared in

140  The Tensor Product of Two Good Codes Is Not Necessarily Robustly Testable

This work presents two linear codes of constant relative distance and constant rate such that their tensor product is not robust.

Credits: Authored by O. Goldreich and O. Meir. Appeared in

141  A Small Gap in the Gap Amplification of Assignment Testers

Irit Dinur’s proof of the PCP theorem via gap amplification has an important extension to Assignment Testers (a.k.a PCPPs). This work points out a gap in the proof of this extension, and shows that this gap can be bridged.

Credits: Authored by O. Goldreich and O. Meir.

142  Algorithmic Aspects of Property Testing in the Dense Graphs Model

This work considers two refined questions regarding the query complexity of testing graph properties in the adjacency matrix model. The first question refers to the relation between adaptive and non-adaptive testers, whereas the second question refers to testability within complexity that is inversely proportional to the proximity parameter. The study of these questions reveals the importance of algorithmic design (also) in this model.

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

143  On Proximity Oblivious Testing

This work initiates a systematic study of a special type of property testers. These testers consist of repeating a basic test for a number of times that depends on the proximity parameters, whereas the basic test is oblivious of the proximity parameter.

Credits: Authored by O. Goldreich and D. Ron. Appeared in
144 Hierarchy Theorems for Property Testing

Referring to the query complexity of property testing, this work establishes the existence of a rich hierarchy of corresponding complexity classes. Such results are proven in three standard domains often considered in property testing: generic functions, adjacency predicates describing (dense) graphs, and incidence functions describing bounded-degree graphs.

Credits: Authored by O. Goldreich, M. Krivelevich, I. Newman, and E. Rozenberg. Appeared in

145 From absolute distinguishability to positive distinguishability

This study refers to methods of converting algorithms that distinguish pairs of distributions with a gap that has an absolute value that is noticeable into corresponding algorithms in which the gap is always positive (and noticeable).

Credits: Authored by Z. Brakerski and O. Goldreich. Appeared in

146 A Candidate Counterexample to the Easy Cylinders Conjecture

This study refers to the easy cylinders conjecture, suggested by Manindra Agrawal and Osamu Watanabe (CCC, 2009).

Credits: Authored by O. Goldreich. Appeared in

147 A Theory of Goal-Oriented Communication

This work puts forward a general theory of goal-oriented communication, where communication is not an end in itself, but rather a means to achieving some goals of the communicating parties. Focusing on goals provides a mechanism for overcoming the problem of potential “misunderstanding” during communication, a protocol for “reliable communication” should overcome any initial misunderstanding between parties and still achieve the goal. The richness of the theory arises from the fact that there is an enormous diversity among the goals of communication. Despite the diversity, a simple model that captures every goal is proposed and studied.

Credits: Authored by O. Goldreich, B. Juba, and M. Sudan. Appeared in
148 More Constructions of Lossy and Correlation-Secure Trapdoor Functions

This work proposes new and improved instantiations of lossy trapdoor functions and correlation-secure trapdoor functions.

Credits: Authored by D. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev. Appeared in

149 Testing Graph Blow-Up

Referring to the query complexity of testing graph properties in the adjacency matrix model, we advance the study of the class of properties that can be tested non-adaptively within complexity that is inversely proportional to the proximity parameter. Specifically, we show that, for every fixed graph $H$, testing whether the graph is a blow-up of $H$ belongs to this class.

Credits: Authored by L. Avigad and O. Goldreich. Appeared in

150 Proximity Oblivious Testing and the Role of Invariances

This work presents a general notion of properties that are characterized by local conditions that are invariant under a sufficiently rich class of symmetries. It shows that in certain models of property testing having such a characterization is closely related to having a proximity oblivious tester, while in others models the two features are orthogonal.

Credits: Authored by O. Goldreich and T. Kaufman. Appeared in

151 Finding Cycles and Trees in Sublinear Time

This work presents sublinear-time (randomized) algorithms for finding simple cycles of length at least $k \geq 3$ and tree-minors in bounded-degree graphs. The complexity of these algorithms is related to the distance of the graph from being $C_k$-minor free (resp., free from having the corresponding tree-minor).

Credits: Authored by A. Czumaj, O. Goldreich, D. Ron, C. Seshadhri, A. Shapira, and C. Sohler. Appeared in

152 On Testing Computability by Small Width OBDDs

This work takes another step in the study of the testability of small-width OBDDs. While testing whether a function $f : \{0,1\}^n \rightarrow \{0,1\}$ is implemented by a width-2 OBDD has query complexity $\Theta(\log n)$, one of the new results is that the analogue problem for width-4 OBDDs has query complexity $\Omega(\sqrt{n})$.

Credits: Authored by O. Goldreich. Appeared in
153  *In a World of P=BPP*

This work shows that proving results such as BPP=P essentially necessitate the construction of suitable pseudorandom generators (i.e., generators that suffice for such derandomization results). It also identify a natural class of search problems that can be solved by deterministic polynomial-time reductions to BPP. This result is instrumental to the construction of the aforementioned pseudorandom generators (based on the assumption BPP=P), which is actually a reduction of the “construction problem” to BPP.

**Credits:** Authored by O. Goldreich. Appeared in


154  *Input-Oblivious Proof Systems and a Uniform Complexity Perspective on P/poly*

This work revisits the notion of input-oblivious proof systems, and initiate a more systematic study of them. In particular, the study is extended to input-oblivious versions of IP, PCP, and ZK.

**Credits:** Authored by O. Goldreich and O. Meir. Appeared in


155  *Two Comments on Targeted Canonical Derandomizers*

This work revisit the notion of a targeted canonical derandomizer, introduced in work Nr. as a uniform notion of a pseudorandom generator that suffices for yielding $BPP = P$. Here we consider pseudorandom generators that fool a single circuit that is given to them as auxiliary input, and show that such pseudorandom generators exist if and only if $BPP = P$.

**Credits:** Authored by O. Goldreich. Appeared in

- ECCC TR11-047, 2011.

**Sabbatical at IAS (2011–12)**

156  *Enhancements of Trapdoor Permutations*

This work takes a closer look at several enhancements of the notion of trapdoor permutations, clarifying why these enhancements are needed in some applications.

**Credits:** Authored by O. Goldreich and R. Rothblum. Appeared in


157  *Monotone Circuits: One-Way Functions versus Pseudorandom Generators*

This work studies the computability of one-way functions and pseudorandom generators by monotone circuits, showing a substantial gap between the two.
158 On the Effect of the Proximity Parameter on Property Testers

It is shown that, except in pathological cases, the effect of the proximity parameter on property testers is effectively restricted to determining the query complexity of the tester.

Credits: Authored by O. Goldreich. Appeared in

159 Two-Sided Error Proximity Oblivious Testing

This work generalizes the notion of Proximity Oblivious Testing, which was originally defined with respect to one-sided error testing, to two-sided error testing.

Credits: Authored by O. Goldreich and I. Shinkar. Appeared in

160 On the possibilities and limitations of pseudodeterministic algorithms

We study the possibilities and limitations of probabilistic algorithms that solve search problems such that on each input, with high probability, they output the same (“canonical”) solution. We consider both the standard setting of (probabilistic) polynomial-time algorithms and the setting of (probabilistic) sublinear-time algorithms.

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

Back at Weizmann (2012–2019)

161 On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions

We propose that multi-linear functions of relatively low degree over GF(2) may be good candidates for obtaining exponential lower bounds on the size of constant-depth Boolean circuits (computing explicit functions). Towards studying this conjecture, we suggest to study two frameworks for the design of depth-three Boolean circuits computing multilinear functions, yielding restricted models for which lower bounds may be easier to prove.

Credits: Authored by O. Goldreich and A. Wigderson. Appeared in
162 On Multiple Input Problems in Property Testing

We study three types of multiple input problems in the context of property testing corresponding to Direct Sum, Direct Product, and Concatenation. We show that the query complexity of the first two problems grows linearly with the number of instances, whereas the complexity of the third problem remain essentially intact.

Credits: Authored by O. Goldreich. Appeared in

163 On the Communication Complexity Methodology for Proving Lower Bounds on the Query Complexity of Property Testing

We present a general formulation of the methodology put forward by Blais, Brody, and Matulef. We advocate the use of the general formulation, because it is easier to apply, while showing that it actually is not more powerful than the original restricted formulation.

Credits: Authored by O. Goldreich. Appeared in

164 On Sample-Based Testers

We advance the study of sample-based property testers by providing several general positive results as well as by revealing relations between variants of this testing model.

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

165 On Derandomizing Algorithms that Err Extremely Rarely

This work puts forward and initializes the study of the following quantified derandomization challenge: For a class of circuits $C$ and a bounding function $B$, given an $n$-input circuit $C$ from $C$ that evaluates to 1 on all but at most $B(n)$ of its inputs, find (in deterministic polynomial-time) an input $x$ such that $C(x) = 1$.

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

166 Strong Locally Testable Codes with Relaxed Local Decoders

This work presents a construction of binary linear codes of nearly-linear length that are both strong-LTCs (with one-sided error) and constant-query relaxed-LDCs.

Credits: Authored by O. Goldreich, T. Gur, and I. Komargodski. Appeared in
167 On Learning and Testing Dynamic Environments

This work initiates a study of learning and testing dynamic environments, focusing on environment that evolve according to a fixed local rule. We focus on the temporal aspect of learning and testing such evolving environments, which is reflected in the requirement that only a small portion of the environment is inspected in each time slot.

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

168 Super-Perfect Zero-Knowledge Proofs

We initiate a study of super-perfect zero-knowledge proof systems, where the interaction can be perfectly simulated in strict probabilistic polynomial-time.

Credits: Authored by O. Goldreich and L. Teichner. Appeared in

169 On Randomness Extraction in AC0

This paper considers the possibility and limitations of randomness extraction by AC0 circuits, examining various models including seeded extractors for general sources and seedless extractors for bit-fixing sources and several independent sources. Credits: Authored by O. Goldreich, E. Viola, and A. Wigderson. Appeared in

170 Proofs of Proximity for Context-Free Languages and Read-Once Branching Programs

This work presents interactive and non-interactive proofs of proximity for two natural classes of properties: (1) context-free languages, and (2) languages accepted by small read-once branching programs.

Credits: Authored by O. Goldreich, T. Gur, and R. Rothblum. Appeared in
- In 42nd ICALP (1), pages 666–677, 2015.

171 Matrix Rigidity of Random Toeplitz Matrices

This work shows that random $n$-by-$n$ Toeplitz matrices over $F_2$ have rigidity $\Omega(\frac{n^2}{r^2 \log n})$ for rank $r \geq \sqrt{n}$. This implies that the explicit trilinear $[n] \times [n] \times [2n]$ function defined by $F(x, y, z) = \sum_{i,j} x_i y_j z_{i+j}$ has complexity $\Omega(n^{3/5})$ in the multilinear circuit model suggested by Goldreich and Wigderson (ECCC, 2013), which yields an exp($n^{3/5}$) lower bound on the size of the so-called canonical depth-three circuits for $F$.

Credits: Authored by O. Goldreich and A. Tal. Appeared in
172 The uniform distribution is complete with respect to testing identity to a fixed distribution

This work presents a reduction of the class of problems consisting of testing whether an unknown distribution over $[n]$ equals a fixed distribution to this very problem when the fixed distribution is uniform over $[n]$.

Credits: Authored by O. Goldreich. Appeared in
- ECCC TR16-015, 2016

173 Universal Locally Testable Codes

This work initiates a study of error correcting codes $C$ that admit the decoding or verification of arbitrary functions of the original message; that is, for a family $\mathcal{F}$ of Boolean functions (of $k$-bit strings), given $f \in \mathcal{F}$ and oracle access to a purported codeword $w \in \{0,1\}^n$, the tester returns either $f(C^{-1}(w))$ or an indication that $w$ is not a valid codeword.

Credits: Authored by O. Goldreich and T. Gur. Appeared in

174 On Emulating Interactive Proofs with Public Coins

This work analyzes a natural alternative to the known emulation of general interactive proof systems by public-coin ones. In this emulation, if the parties play honestly, then each message is selected with probability that approximately equals the probability that it is selected in the original protocol.

Credits: Authored by O. Goldreich and M. Leshkowitz. Appeared in
- ECCC TR16-066, 2016.

175 Reducing testing affine spaces to testing linearity

We show that testing whether a Boolean function $f : \{0,1\}^\ell \to \{0,1\}$ is the indicator function of an $(\ell - k)$-dimensional affine space can be reduced to the linearity of a related function $g : \{0,1\}^\ell \to \{0,1\}^k$, rather than by a cumbersome generalization of the ideas used in the celebrated linearity tester (of Blum, Luby and Rubinfeld (JCSS, 1993)).

Credits: Authored by O. Goldreich. Appeared in
- ECCC TR16-080, 2016
176 Deconstructing 1-local expanders

Starting from a generic candidate for a 1-local expander, we formulate a natural problem regarding coordinated random walks (CRW) on the corresponding relocation graph (which has size that is logarithmic in the size of the candidate 1-local graph), and observe that (1) any solution to the CRW problem yields 1-local expanders, and (2) any constant-size expanding set of generators for the symmetric group yields a solution to the CRW problem.

Credits: Authored by O. Goldreich. Appeared in
- ECCC TR16-152, 2016

177 Universal Locally Verifiable Codes and 3-Round Interactive Proofs of Proximity for CSP

In continuation to the work on Universal Locally Testable Codes, this work initiates a study of the proof-based version of this notion.

Credits: Authored by O. Goldreich and T. Gur. Appeared in
- ECCC TR16-192, 2016

178 Simple doubly-efficient interactive proof systems for locally-characterizable sets

A proof system is called doubly-efficient if the prescribed prover strategy can be implemented in polynomial-time and the verifier’s strategy can be implemented in almost-linear-time. We present direct constructions of doubly-efficient interactive proof systems for problems in $P$ that are believed to have relatively high complexity. In particular, we present a generic construction of such proof systems for a natural class that contains the problems $t$-CLIQUE and $t$-SUM and is in NC (and also in SC).

Credits: Authored by O. Goldreich and G. Rothblum. Appeared in

179 Worst-case to Average-case reductions for subclasses of $P$

For every polynomial $q$, we present worst-case to average-case (almost-linear-time) reductions for a class of problems in $P$ that are widely conjectured not to be solvable in time $q$. This class consists of problems that call for counting the number of local neighborhoods in the input that satisfy some predetermined conditions, where the number of neighborhoods is polynomial, and the neighborhoods as well as the conditions can be specified by small uniform Boolean formulas.

Credits: Authored by O. Goldreich and G. Rothblum. Appeared in
- ECCC TR17-130, 2017
180 On Constant-Depth Canonical Boolean Circuits for Computing Multilinear Functions

We consider new complexity measures for the model of multilinear circuits with general multilinear gates introduced by Goldreich and Wigderson (2013). These complexity measures are related to the size of canonical constant-depth Boolean circuits, which extend the definition of canonical depth-three Boolean circuits.

Credits: Authored by O. Goldreich and A. Tal. Appeared in
- ECCC TR17-193, 2017

181 The Subgraph Testing Model

We initiate a study of testing properties of graphs that are presented as subgraphs of a fixed (or an explicitly given) graph. The tester is given free access to a base graph $G = ([n], E)$, and oracle access to a function $f : E \rightarrow \{0, 1\}$ that represents a subgraph of $G$. The tester is required to distinguish between subgraphs that possess a predetermined property and subgraphs that are far from possessing this property.

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

182 Counting $t$-cliques: Worst-case to average-case reductions and Direct interactive proof systems

We present two main results regarding the complexity of counting the number of $t$-cliques in a graph. (1) A reduction of counting $t$-cliques in any $n$-vertex graph to counting $t$-cliques in typical $n$-vertex graphs that are drawn from a simple distribution. (2) A direct and simple doubly-efficient interactive proof system for counting $t$-cliques in $n$-vertex graphs.

Credits: Authored by O. Goldreich and G. Rothblum. Appeared in

183 Every set in P is strongly testable under a suitable encoding

We show that every set in P is strongly testable under a suitable encoding. By “strongly testable” we mean having a (proximity oblivious) tester that makes a constant number of queries and rejects with probability that is proportional to the distance of the tested object from the property. By a “suitable encoding” we mean one that is polynomial-time computable and invertible. This result stands in contrast to the known fact that some sets in P are extremely hard to test, providing another demonstration of the crucial role of representation in the context of property testing.

Credits: Authored by I. Dinur, O. Goldreich, and T. Gur. Appeared in
184 Constant-round interactive proof systems for AC0[2] and NC1

We present constant-round interactive proof systems for sufficiently uniform versions of AC0[2] and NC1. Both proof systems are doubly-efficient, and offer a better trade-off between the round complexity and the total communication than known before.

Credits: Authored by O. Goldreich and G. Rothblum. Appeared in

185 Hierarchy Theorems for Testing Properties in Size-Oblivious Query Complexity

Focusing on property testing tasks that have query complexity that is independent of the size of the tested object (i.e., depends on the proximity parameter only), we prove the existence of a rich hierarchy of the corresponding complexity classes. Such results are proved in three standard domains that are often considered in property testing: generic functions, adjacency predicates describing (dense) graphs, and incidence functions describing bounded-degree graphs.

Credits: Authored by O. Goldreich. Appeared in

186 Flexible models for testing graph properties

The standard models of testing graph properties postulate that the vertex-set consists of \{1, 2, ..., n\}, where \(n\) is a natural number that is given explicitly to the tester. Here we suggest more flexible models by postulating that the tester is given access to samples the arbitrary vertex-set; that is, the vertex-set is arbitrary, and the tester is given access to a device that provides uniformly and independently distributed vertices. In addition, the tester may be (explicitly) given partial information regarding the vertex-set (e.g., an approximation of its size).

Credits: Authored by O. Goldreich. Appeared in

187 Testing Graphs in Vertex-Distribution-Free Models

Prior studies of testing graph properties presume that the tester can obtain uniformly distributed vertices in the tested graph (in addition to obtaining answers to the some type of graph-queries). Here we envision settings in which it is only feasible to obtain random vertices drawn according to an arbitrary distribution (and, in addition, obtain answers to the usual graph-queries). We initiate a study of testing graph properties in such settings, while adapting the definition of distance between graphs so that it reflects the different probability weight of different vertices.

Credits: Authored by O. Goldreich. Appeared in
188 Multi-pseudodeterministic algorithms

This work relaxes the notion of pseudodeterminism by allowing the algorithms to output one of a bounded number of canonical solutions (per each input), and initiates a study of this relaxation.

Credits: Authored by O. Goldreich. Appeared in

189 Testing Bipartitness in an Augmented VDF Bounded-Degree Graph Model

Augmenting the foregoing Vertex-Distribution-Free model, by providing the tester with an evaluation oracle to the unknown distribution $D$, testers are presented for Bipartitness and cycle-freeness in bounded-degree graphs.

Credits: Authored by O. Goldreich. Appeared in

190 Pseudo-Mixing Time of Random Walks

This work introduces the notion of pseudo-mixing time of a graph defined as the number of steps in a random walk that suffices for generating a vertex that looks random to any polynomial-time observer, where, in addition to the tested vertex, the observer is also provided with oracle access to the incidence function of the graph. Assuming the existence of one-way functions, it is shown that the pseudo-mixing time of a graph can be much smaller than its mixing time.

Credits: Authored by I. Benjamini and O. Goldreich. Appeared in

191 On the Complexity of Estimating the Effective Support Size

This work studies the complexity of estimating the effective support size of an unknown distribution when given samples of the distributions as well as an evaluation oracle, and presents several algorithms that exhibit a trade-off between the quality of the approximation and the complexity of obtaining it.

Credits: Authored by O. Goldreich. Appeared in

192 Testing Isomorphism in the Bounded-Degree Graph Model

This work determines the query complexity of testing isomorphism to a fixed graph and between two unknown graphs in the special case of graphs with connected components of poly-logarithmic size.

Credits: Authored by O. Goldreich. Appeared in
Sabbatical at Columbia (2019–20)

193 Improved bounds on the AN-complexity of multilinear functions

Credits: Authored by O. Goldreich. Appeared in

194 Randomness Extraction from Somewhat Dependent Sources

This work initiates a comprehensive study of the question of randomness extractions from two somewhat dependent sources of defective randomness. It present and studies three natural models, which are based on different natural perspectives on the notion of bounded dependency between a pair of distributions.

Abstract (abbr.): Going from the more restricted model to the less restricted one, the models and main results are as follows.

- Bounded dependence as bounded coordination: Here we consider pairs of distributions that arise from independent random processes that are applied to the outcome of a single global random source. It is shown that if the min-entropy of each of the two outcomes is larger than the length of the global source, then (seedless) extraction is possible (and is, in fact, feasible).

- Bounded dependence as bounded cross influence: Here we consider pairs of outcomes that are produced by a pair of sources such that each source has bounded (worst-case) influence on the outcome of the other source. Its is showm that, while (proper) randomness extraction is impossible in this case, randomness condensing is possible and feasible. Various applications of such condensers, including for cryptography, standard randomized algorithms, and sublinear-time algorithms, are discussed, while pointing out their benefit over using a seeded (single-source) extractor.

- Bounded dependence as bounded mutual information: Due to the average-case nature of this mutual information, here there is a trade-off between the error (or deviation) probability and the randomness deficiency.

All positive results are obtained by using a standard two-source extractor (or condenser) as a black-box.

Credits: Authored by M. Ball, O. Goldreich, and T. Malkin. Appeared in

195 Communication Complexity with Defective Randomness

This work studies the public-randomness and private-randomness models when the commonly postulated perfect randomness is replaced by distributions with bounded min-entropy deficiency.
196 One-Sided Error Testing of Monomials and Affine Subspaces

The point here is obtaining one-sided testers for these properties, whereas prior work presented two-sided error testers.

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

197 On Counting $t$-Cliques Mod 2

For a constant integer $t$, this work presents a simple worst-case to average-case reduction for counting $t$-cliques mod 2, where average-case is with respect to the uniform distribution over graphs with a given number of vertices.

Credits: Authored by O. Goldreich. Appeared in

198 On Testing Hamiltonicity in the Bounded Degree Graph Model

It is shown that the query complexity of testing Hamiltonicity in the bounded degree graph model is linear.

Credits: Authored by O. Goldreich. Appeared in

199 On Testing Asymmetry in the Bounded Degree Graph Model

This work initiates a study of the query complexity of testing the property of being an asymmetric graph.

Credits: Authored by O. Goldreich. Appeared in

200 Robustly Self-Ordered Graphs: Constructions and Applications to Property Testing

We say that $G = (V, E)$ is robustly self-ordered if the size of the symmetric difference between $E$ and the edge-set of the graph obtained by permuting $V$ using any permutation $\pi : V \to V$ is proportional to the number of non-fixed-points of $\pi$. We present constructions of robustly self-ordered graphs both in the bounded-degree and dense graph regimes, where in both cases the foregoing proportion (robustness parameter) is required to be linear in the maximum degree.

Credits: Authored by O. Goldreich and A. Wigderson. Appeared in
Non-adaptive vs Adaptive Queries in the Dense Graph Testing Model

It has been known for a couple of decades that the query complexity of non-adaptive testers is at most quadratic in the query complexity of adaptive testers. We show that this general result is essentially tight; that is, there exist graph properties for which any non-adaptive tester must have query complexity that is almost quadratic in the query complexity of the best general (i.e., adaptive) tester.

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

Constructing Large Families of Pairwise Far Permutations: Good Permutation Codes Based on the Shuffle-Exchange Network

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