List of Publications

Oded Goldreich

January 3, 2019

Contents

1 Theses 1

2 Original Papers in Refereed Journals 1

3 Original Papers in (Refereed) Conference Proceedings 7

4 Other Work 16

4.1 Collected Works (LNCS Vol. 6650, 2011) 16

4.2 Papers in Electronic Forum 17

4.3 Reports and Unpublished Manuscripts 19

5 Survey Papers 19

5.1 Chapters in Books 19

5.2 Published in Periodicals or Conference Proceedings 20

5.3 Collected Works (LNCS Vol. 6650, 2011) 21

5.4 Electronic posting 22

6 Books, Lecture Notes, and Related Material 22
1 Theses


  Thesis adviser: Prof. S. Even, 1983.

2 Original Papers in Refereed Journals

Published


Accepted

[J92] O. Goldreich, T. Gur, and I. Komargodski. Strong Locally Testable Codes with Relaxed Local Decoders, ACM Transactions on Computation Theory,
3 Original Papers in (Refereed) Conference Proceedings

The paper are ordered by the date of the conferences, and not by the date of the publication of its proceedings. This comment is relevant with respect to the early Crypto’ conferences (i.e., of the 1980’s). Also, till the late 1980’s, simultaneous publication in various conferences was allowed (and even encouraged).


[C18] B. Chor and O. Goldreich, Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity, Proc. of the 26th IEEE Symp. on Foundation of Computer Science (FOCS), 1985, pp. 429-442. (This is an extended abstract of No. J9.)


on Foundation of Computer Science (FOCS), pp. 174-187, 1986. (This is an extended abstract of No. J18.)


[C35] S. Ben-David, B. Chor, O. Goldreich, and M. Luby, On the Theory of Average Case Complexity, Proc. of the 4th conf. on Structure in Complexity Theory, (This is an abstract of No. C37.)


[C40] O. Goldreich, and H. Krawczyk, On Sparse Pseudorandom Ensembles, Advances in Cryptology – Crypto ’89 (Proceedings), Lecture Note in Computer Science (435) Springer Verlag, pp. 113–127, 1990. (This is an extended abstract of No. J22.)


[C60] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, Private Information Retrieval, 
41-50, 1995. (This is an extended abstract of No. J46.)

[C61] M. Bellare, O. Goldreich and M. Sudan, Free Bits and Non-Approximability, 
422-431, 1995. (This is an extended abstract of No. J41.)

[C62] O. Goldreich, R. Rubinfeld and M. Sudan, Learning polynomials with queries: the 
highly noisy case, Proc. of the 36th IEEE Symp. on Foundation of Computer 
Science (FOCS), pp. 294-303, 1995. (This is an extended abstract of No. J57.)

[C63] R. Canetti, U. Feige, O. Goldreich and M. Naor, Adaptively Secure Multi-party Compu-
tation, Proc. of the 28th ACM Symp. on Theory of Computing (STOC), pp. 639-648, 
1996.

[C64] O. Goldreich, S. Goldwasser and D. Ron, Property Testing and its connection to Learn-
 ing and Approximation, Proc. of the 37th IEEE Symp. on Foundation of Computer 
Science (FOCS), pp. 339-348, 1996. (This is an extended abstract of No. J44.)

[C65] O. Goldreich and D. Ron, Property Testing in Bounded Degree Graphs, Proc. of the 
29th ACM Symp. on Theory of Computing (STOC), pp. 406-415, 1997. (This is an 
extended abstract of No. J59.)

[C66] S. Decatur, O. Goldreich, and D. Ron, Computational Sample Complexity, 10th COLT, 
pp. 130-142, 1997. (This is a preliminary version of No. J52.)

[C67] O. Goldreich and S. Safra, A Combinatorial Consistency Lemma with application to the 
PCP Theorem, proceedings of Random97, Springer LNCS, Vol. 1269, pp. 67–84. (This 
is a preliminary version of No. J53.)

[C68] O. Goldreich, S. Goldwasser and S. Halevi, Public-Key Cryptosystems from Lattice 

[C69] O. Goldreich, S. Goldwasser and S. Halevi, Eliminating Decryption Errors in the Ajtai-

[C70] O. Goldreich and S. Goldwasser, On the Limits of Non-Approximability of Lattice Prob-
 lems, in Proc. of the 30th ACM Symp. on Theory of Computing (STOC), pp. 1–9, 
1998. (This is an extended abstract of No. J54.)

[C71] O. Goldreich and D. Ron, A Sublinear Bipartitness Tester for Bounded Degree Graphs, 
in Proc. of the 30th ACM Symp. on Theory of Computing (STOC), pp. 289–298, 
1998. (This is an extended abstract of No. J49.)

[C72] R. Canetti, O. Goldreich and S. Halevi, The Random Oracle Methodology, Revisited, 
in Proc. of the 30th ACM Symp. on Theory of Computing (STOC), pp. 209–218, 
1998. (This is an extended abstract of No. J64.)

[C73] O. Goldreich, A. Sahai and S. Vadhan, Honest-Verifier Statistical Zero-Knowledge 
Equals General Statistical Zero-Knowledge, in Proc. of the 30th ACM Symp. on Theory 
[C74] O. Goldreich and M. Sudan, Computational Indistinguishability: A Sample Hierarchy, proceedings of 13th IEEE Conference on Computational Complexity, pages 24-33, 1998. (This is an extended abstract of No. J51.)


[C76] O. Goldreich, S. Goldwasser, E. Lehman and D. Ron, Testing Monotonicity, in 39th FOCS, pages 426–435, 1998. (This extended abstract has been merged with an improvement obtained in joint work with Alex Samorodnitsky to yield No. J56.)

[C77] O. Goldreich, D. Ron and M. Sudan, Chinese Remaindering with Errors, in 31st STOC, pages 225–234, 1999. (This is an extended abstract of No. J55.)


[C87] O. Goldreich and Y. Lindell, Session-Key Generation using Human Passwords Only, Proceedings of Crypto01, pages 408–432. (This is an extended abstract of No. J66.)

13
B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, On the (Im)possibility of Software Obfuscation, Proceedings of Crypto’01, pages 1–18. (This is an extended abstract of No. J80.)


O. Goldreich and L. Trevisan, Three Theorems regarding Testing Graph Properties, in Proc. of the 42th FOCS, pages 460–469, 2001. (This is an extended abstract of No. J63.)

O. Goldreich, Concurrent Zero-Knowledge With Timing, Revisited, in Proc. of the 34th STOC, pages 332–340, 2002. (This is an extended abstract of No. J65.)


B. Barak and O. Goldreich, Universal arguments and their applications, in the proceedings of 17th IEEE Conference on Computational Complexity, pages 194–203, 2002. (This is an extended abstract of No. J71.)

O. Goldreich and A. Wigderson, Derandomization that is rarely wrong from short advice that is typically good, in the proceedings of RANDOM, Springer LNCS, Vol. 2483, pages 209–223, 2002.

O. Goldreich and M. Sudan, Locally Testable Codes and PCPs of Almost-Linear Length, in Proc. of the 43rd FOCS, pages 13–22, 2002. (This is an extended abstract of No. J67.)


E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Robust PCPs of Proximity, Shorter PCPs and Applications to Coding, in Proc. of the 36th STOC, pages 1-10, 2004. (This is an extended abstract of No. J69.)


O. Goldreich and D. Ron, Approximating Average Parameters of Graphs, in the proceedings of 10th RANDOM, Springer LNCS, Vol. 4110, pages 363–374, 2006. (This is an extended abstract of No. J70.)
4 Other Work

This section only lists works that are not listed in the prior sections. Likewise, works are listed in the first relevant subsection. In all cases, these publications were not refereed.

4.1 Collected Works (LNCS Vol. 6650, 2011)

The works collected in this volume were completed at different times, and were revised towards this publication. The year of the original version is mentioned in square brackets.


[O6] O. Goldreich and D. Zuckerman, Another proof that BPP subseteq PH (and more) [1997]


[O10] O. Goldreich, Candidate One-Way Functions Based on Expander Graphs [2000]

[O11] O. Goldreich, Using the FGLSS-reduction to Prove Inapproximability Results for Minimum Vertex Cover in Hypergraphs [2001]


[O16] O. Goldreich, A Candidate Counterexample to the Easy Cylinders Conjecture [2009]

[O17] Z. Brakerski and O. Goldreich, From absolute distinguishability to positive distinguishability [2009]


4.2 Papers in Electronic Forum


[O30] O. Goldreich. The uniform distribution is complete with respect to testing identity to a fixed distribution, ECCC TR16-015, 2016.


4.3 Reports and Unpublished Manuscripts

Research Reports

[O44] O. Goldreich, Graph Partition into Equinumerous Connected Components is NP-Complete, TR No. 202, Computer Science Department, Technion, Haifa, Israel, 1981.


Unpublished Manuscripts (cited by other researchers)


5 Survey Papers

5.1 Chapters in Books


### 5.2 Published in Periodicals or Conference Proceedings


[S19] Pseudorandomness, in *Notices of AMS*, pages 1209–1216, November 1999. (This is an abbreviated version of No. S20.)


Zero-Knowledge: Abstract of a Tutorial, in the Proc. of the 43rd FOCS, page 3, 2002. (This is an abstract of No. S23.)


5.3 Collected Works (LNCS Vol. 6650, 2011)

In addition to the surveys listed next, surveys number S9, S11, S12, and S25 also appear in this collection. The surveys collected in this volume were completed at different times, and were revised towards this publication. The year of the original version is mentioned in square brackets.

On Yao’s XOR-Lemma (with N. Nisan and A. Wigderson) [1995]

Three XOR-Lemmas – An Exposition [1995]

A Sample of Samplers – A Computational Perspective on Sampling [1997]

Notes on Levin’s Theory of Average-Case Complexity [1988 and 1997]


On the complexity of computational problems regarding distributions (with S. Vadhan) [2003]

Basing Non-Interactive Zero-Knowledge on (Enhanced) Trapdoor Permutations: The State of the Art [2008]

Average Case Complexity, Revisited [2008]

Basic Facts about Expander Graphs [2008]

A Brief Introduction to Property Testing [2010]
5.4 Electronic posting

ECCC resides at http://www.eccc.uni-trier.de/eccc/.


6 Books, Lecture Notes, and Related Material

Books


Lecture Notes


(Superseded by B2 and B3.)


2. For a one-semester course, 104 pages, 2002.

Department of Computer Science and Applied Math., Weizmann Institute of Science. (Superseeded by B4.)

Department of Computer Science and Applied Math., Weizmann Institute, 155 pages.

Other Material

Department of Computer Science and Applied Math., Weizmann Institute, 292 pages.
(This is a preliminary version of B2.)