# List of Publications

Oded Goldreich

January 24, 2014

## Contents

1. Theses ........................................ 1

2. Original Papers in Refereed Journals .......................... 1

3. Original Papers in (Refereed) Conference Proceedings .............. 6

4. Other Work .................................... 15
   4.1 Collected Works (LNCS Vol. 6650, 2011) .................... 15
   4.2 Papers in Electronic Forum .................................. 16
   4.3 Reports and Unpublished Manuscripts ........................ 17

5. Survey Papers .................................. 18
   5.1 Chapters in Books ......................................... 18
   5.2 Published in Periodicals or Conference Proceedings ............ 19
   5.3 Collected Works (LNCS Vol. 6650, 2011) .................... 20

1 Theses


  Thesis adviser: Prof. S. Even, 1983.

2 Original Papers in Refereed Journals

Published


In Press


Submitted

[J85] O. Goldreich and I. Shinkar. Two-Sided Error Proximity Oblivious Testing,

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.)


[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.)


[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.)


[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.)


[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.)

[C88] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, On the (Im)possibility of Software Obfuscation, Proceedings of Crypto01, pages 1–18. (This is an extended abstract of No. J80.)


[C90] 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.)

[C91] 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.)


[C95] 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.)


[C99] 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, On Proximity Oblivious Testing, Proceedings of the 41st STOC, pages 141–150, 2009. (This is an extended abstract of No. J76.)

O. Goldreich and D. Ron, Algorithmic Aspects of Property Testing in the Dense Graphs Model, in the proceedings of 13th RANDOM, Springer LNCS, Vol. 5687, pages 520–533, 2009. (This is an extended abstract of No. J75.)


O. Goldreich, B. Juba, and M. Sudan, A Theory of Goal-Oriented Communication, in the proceedings of 30th PODC, pages 299–300, 2011. (This version is related to No. JJ:GJS.)


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.
[O1] O. Goldreich, Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle is NP-Hard, [1984]


[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]

[O18] O. Goldreich. In a World of P=BPP, [2010]

4.2 Papers in Electronic Forum


4.3 Reports and Unpublished Manuscripts

Research Reports


Unpublished Manuscripts  (cited by other researchers)


5 Survey Papers

5.1 Chapters in Books


5.2 Published in Periodicals or Conference Proceedings


(A brief summary has appeared in *CryptoBytes*, the technical newsletter of RSA Laboratories, Vol. 3, No. 2, 1997.)

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


[S22] 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.

[S33] On the complexity of computational problems regarding distributions, (with S. Vadhan) [2003]
[S34] Basing Non-Interactive Zero-Knowledge on (Enhanced) Trapdoor Permutations: The State of the Art, [2008]
[S35] Average Case Complexity, Revisited, [2008]
[S36] Basic Facts about Expander Graphs, [2008]
[S37] A Brief Introduction to Property Testing, [2010]

6 Books, Lecture Notes, and Related Material

Books


Lecture Notes

    Computer Science Department, Technion, 184 pages.
    (Superseeded by B2 and B3.)

    Computer Science Department, Technion, 184 pages. (Third edition: 1992.)

    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.)