Work and Publications

Oded Goldreich

January 14, 2020


  • Advances in Cryptology: Proceedings of Eurocrypt84, (T. Beth et. al. eds.), Lecture

    464-479.
  • Reprinted in Providing Sound Foundations for Cryptography, pages 241–264, 2019

  • Unpublished manuscript, July 1984.

  • Unpublished manuscript, October 1984.

  • Advances in Cryptology: Proceedings of Eurocrypt84, (T. Beth et. al. eds.), Lecture

    As Hard As the Whole.
    449-457.
  • (partial result w/ B. Chor only), Advances in Cryptology – Crypto ‘84 (Proceedings),

    Functions.
  • Advances in Cryptology – Crypto ’84 (Proceedings), (G.R. Blakely et. al. eds.), Lecture


    Failures – The Case of a Ring.


  • Proc. of the 26th IEEE Symp. on Foundation of Computer Science (FOCS), 1985, pp. 429-442.


  • Algorithmica, 5, pp. 1–10, 1990.

  • Proc. of the 12th International Colloquium on Automata Languages and Programming (ICALP), Lecture Note in Computer Science (194) Springer Verlag, 1985, pp. 43-52.


[25] O. Goldreich, Two Remarks Concerning the GMR Signature Scheme.

[26] O. Goldreich, S. Micali, and A. Wigderson, Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs.

[27] O. Goldreich, Towards a Theory of Software Protection and Simulation by Oblivious RAMs.


[28] O. Goldreich, S. Micali, and A. Wigderson, How to Play any Mental Game or a Completeness Theorem for Protocols with Honest Majority.


[43] O. Goldreich, A Note on Computational Indistinguishability.
[44] O. Goldreich and E. Petrank, Quantifying Knowledge Complexity.


○ Theory of Cryptography Library, record Arc-03.


  • *ECCC*, TR95-050, 1995.


[75] O. Goldreich, S. Goldwasser and D. Ron, Property Testing and its connection to Learning and Approximation.


[81] O. Goldreich, The Graph Clustering Problem has a Perfect Zero-Knowledge Proof.
    • ECCC, TR96-054, November 1996.


    • 10th COLT, pp. 130-142, 1997.


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

    • 13th IEEE Conference on Computational Complexity, pages 24-33, 1998.


[97] O. Goldreich and S. Vadhan, Comparing Entropies in Statistical Zero-Knowledge with Applications to the Structure of SZK.


[98] M. Bellare, O. Goldreich and H. Krawczyk, Beyond the Birthday Barrier, Without Counters.


[100] O. Goldreich, D. Micciancio, S. Safra, and J.P. Seifert, Approximating shortest lattice vectors is not harder than approximating closest lattice vectors.


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


- Proceedings of Crypto01, pages 1–18.


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


[120] O. Goldreich and M. Sudan, Locally Testable Codes and PCPs of Almost-Linear Length.

[121] O. Goldreich and A. Wigderson, Derandomization that is rarely wrong from short advice that is typically good.


   ○ ECCC, TR02-047, 2002.


  ◦ In the proceedings of *20th IEEE Conference on Computational Complexity*, pages 120–134, 2005.


[137] K. Barhum, O. Goldreich and A. Shraibman, On approximating the average distance between points.


[143] Z. Brakerski and O. Goldreich, From absolute distinguishability to positive distinguishability.
   • ECCC, Report TR09-031, Apr. 2009

[144] O. Goldreich, A Candidate Counterexample to the Easy Cylinders Conjecture.
   • ECCC, Report TR09-028, Apr. 2009


   • *Journal of Crypto.*, Online First, 10-Nov-2011.


[151] O. Goldreich. In a World of P=BPP.


  - ECCC TR11-047, 2011.


- Journal of Cryptology, Online First, 12-Sept-2012.


Proceedings of 18th RANDOM, 2014.

   • ECCC TR13-073, 2013.

   • TOCT, Vol. 8(2), 2016.


   • ECCC TR14-097, 2014.


   • In 42nd ICALP (1), pages 666–677, 2015.

   • In 48th STOC, pages 91–104, 2016.

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

• CJTCS, Vol. 2018, Art. 3.

  ○ ECCC TR16-066, 2016.

  ○ ECCC TR16-080, 2016

  ○ ECCC TR16-152, 2016

[175] O. Goldreich and T. Gur. Universal Locally Verifiable Codes and 3-Round Interactive Proofs of Proximity for CSP.
  ○ ECCC TR16-192, 2016


[177] O. Goldreich and G. Rothblum. Worst-case to Average-case reductions for subclasses of P.
  ○ ECCC TR17-130, 2017

  ○ ECCC TR17-193, 2017


  ○ ECCC TR18-069, 2018.

   • ECCC TR18-104, 2018.


   • ECCC TR19-012, 2019.


   • ECCC TR19-078, 2019.

   • ECCC TR19-088, 2019.

   • ECCC TR19-102, 2019.

   • ECCC TR19-171, 2019.

   • ECCC TR19-183, 2019.