Brief Professional Biography

Oded Goldreich

January 30, 2019

Current Position: Professor of Computer Science, Faculty of Mathematical Sciences, Weizmann Institute of Science, Rehovot, Israel. Incumbent of the Meyer W. Weisgal Professorial Chair.

Education, Positions, and Fellowships

Oded Goldreich was born in Tel-Aviv, Israel, on February 4th 1957. Received B.A., M.Sc., and D.Sc. in Computer Science from the Technion (Israel Institute of Technology), Israel, in 1980, 1982, and 1983, respectively. He was a post-doctoral fellow in MIT's Laboratory for Computer Science (1983–86), and a faculty member of the Computer Science Department of the Technion (1983–94). Since March 1994, he is a faculty member of the Computer Science and Applied Mathematics Department of the Weizmann Institute of Science. (He is a Full Professor since 1995, and incumbent of the Weisgal Professorial Chair since 1998).

Oded Goldreich visited MIT (1995–98), and was a *Visiting Miller Research Professor* at the University of California at Berkeley (1996), and a *Fellow of the Radcliffe Institute for Advanced Study* at Harvard University (2003–04). He is a member of the *TCS Chair Professor Team* of Tsinghua University (since 2007).

Oded Goldreich is a *Corresponding Fellow of the Bavarian Academy of Sciences and Humanities* (since 2003), a *Fellow of the International Association for Cryptologic Research* (since 2009), and received the *RSA Conference 2006 Award for Excellence in the Field of Mathematics* and the *2017 Donald E. Knuth prize for fundamental and lasting contributions to theoretical computer science*.

Editorial work, workshop organization, and invited speaker

Oded Goldreich is an associate editor of the journal *Computational Complexity* (since 2003). He was an editor of *SIAM Journal on Computing* (1996–2010) and *Journal of Cryptology* (1992–2011).

Oded Goldreich is a member of the editorial board of *Foundations and Trends in Theoretical Computer Science* (since foundation in 2004) and of the *Electronic Colloquium on Computational Complexity* (since foundation in 1994).

Oded Goldreich was a founding member of the steering committee of the *Theory of Cryptography Conference* and served as chair of this committee (2005–13). He was a co-organizer of the *Complexity Theory Meeting* at Oberwolfach, Germany (1996–2018).

Oded Goldreich was an invited speaker at various conferences including the *International Congress of Mathematicians (ICM) 1994* and the *Crypto97* conference.

Books and Research Contributions

Oded Goldreich is the author of several books, including *Modern Cryptography, Probabilistic Proofs and Pseudorandomness* (Springer 1999), *Foundations of Cryptography: Volumes 1 and 2* (Cambridge University Press, 2001 and 2004), *Computational Complexity: A Conceptual Perspective* (Cambridge University Press, 2008), *P, NP, and NP-Completeness: The Basics of Complexity Theory* (Cambridge University Press, 2010), and *Introduction to Property Testing* (Cambridge University Press, 2017).

Oded Goldreich has published approximately thirty surveys on a range of topics in the theory of computation, and over 160 research papers. His research contributions focus on a variety of subjects related to randomized computations (e.g., *pseudorandom generators*, *probabilistic proof systems*, and *property testing*) and to cryptography (e.g., *zero-knowledge* and *secure multi-party comnputation*). His contributions include

- Showing how to construct zero-knowledge proof systems for any language in NP, using any commitment scheme.
- Showing how to solve any multi-party protocol problem, using any trapdoor permutation.
- Presenting a generic hardcore predicate for any one-way function.
- Showing how to construct pseudorandom functions from any pseudorandom generators.
- Initiating a systematic study of property testing, and advancing its developement in subsequent works.
- Studying various and numerous aspects of pseudorandomness, zero-knowledge proofs, interactive proofs, and probabilistically checkable proofs (PCPs). For example, contructing small-bias sample spaces, advocating the applicability of pairwise independence generators, constructing two-source randomness extractors, introducing the Long-Code as a basic building block of PCPs.

In addition, he made contributions to distributed computing and to other areas of the theory of computation.