Studies in Complexity and Cryptography

This book presents a collection of 36 pieces of scientific work in the areas of complexity theory and foundations of cryptography: 20 research contributions, 13 survey articles, and 3 programmatic and reflective viewpoint statements. These so far formally unpublished pieces were written by Oded Goldreich, some in collaboration with other scientists.

The articles included in this book essentially reflect the topical scope of the scientific career of Oded Goldreich now spanning three decades. In particular the topics dealt with include average-case complexity, complexity of approximation, derandomization, expander graphs, hashing functions, locally testable codes, machines that take advice, NP-completeness, one-way functions, probabilistically checkable proofs, proofs of knowledge, property testing, pseudorandomness, randomness extractors, sampling, trapdoor permutations, zero-knowledge, and non-iterative zero-knowledge.

All in all, this potpourri of studies in complexity and cryptography constitutes a most valuable contribution to the field of theoretical computer science centered around the personal achievements and views of one of its outstanding representatives.

In parallel to the printed book, each new volume is published electronically in LNCS Online.

Detailed information on LNCS can be found at
www.springer.com/lncs
Proposals for publication should be sent to
LNCS Editorial, Tiergartenstr. 17, 69121 Heidelberg, Germany
E-mail: lncs@springer.com

ISSN 0302-9743

ISBN 978-3-642-22669-4

Lecture Notes in Computer Science
LNCS LNAI LNBI

springer.com

Goldreich et al.

LNCS 6650

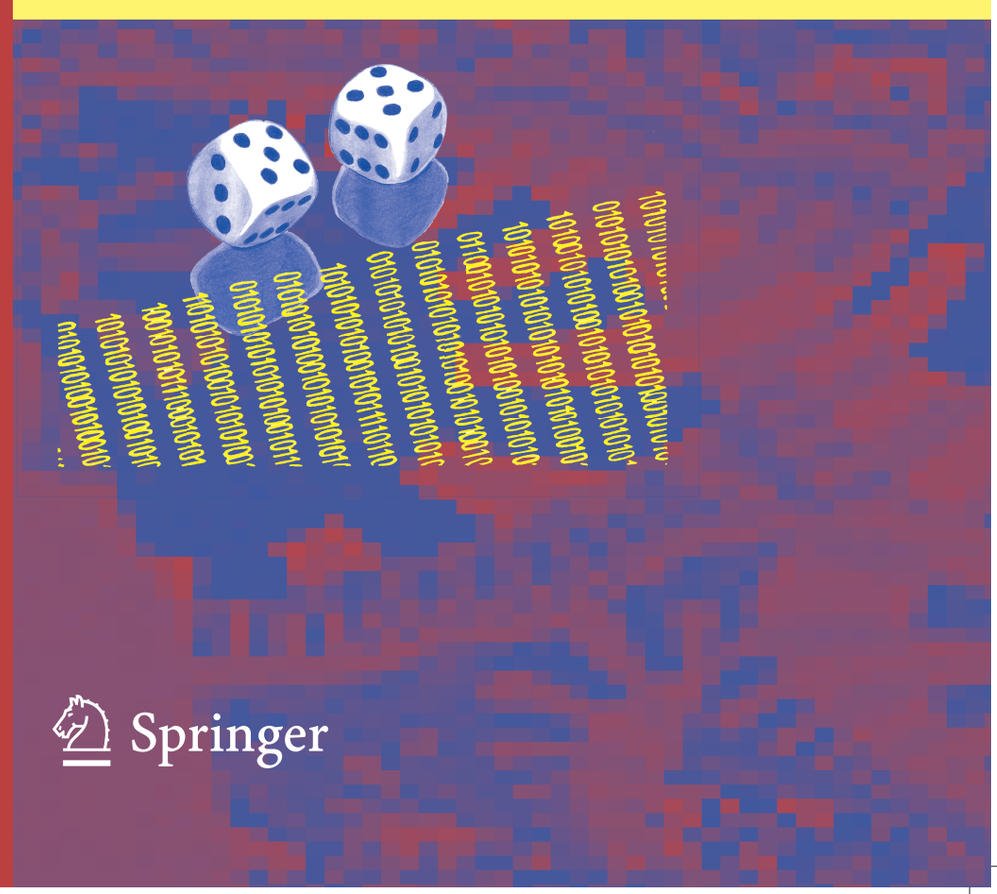
State-of-the-Art Survey

Studies in Complexity and Cryptography

Oded Goldreich et al.

Studies in Complexity and Cryptography

Miscellanea on the Interplay between Randomness and Computation



Springer