

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Oded Goldreich et al.

Studies in Complexity and Cryptography

Miscellanea on the Interplay
between Randomness and Computation

In Collaboration with

Lidor Avigad, Mihir Bellare, Zvika Brakerski

Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin

Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan

Salil Vadhan, Avi Wigderson, David Zuckerman



Springer

Volume Editor

Oded Goldreich
Weizmann Institute of Science
Faculty of Mathematics and Computer Science
76100 Rehovot, Israel
E-mail: oded.goldreich@weizmann.ac.il

Cover illustration: Artwork by Harel Luz, Tel Aviv, Israel.

ISSN 0302-9743	e-ISSN 1611-3349
ISBN 978-3-642-22669-4	e-ISBN 978-3-642-22670-0
DOI 10.1007/978-3-642-22670-0	
Springer Heidelberg Dordrecht London New York	

Library of Congress Control Number: 2011932979

CR Subject Classification (1998): F.1, E.3, E.1, F.4.1, G.2.2, G.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

© Springer-Verlag Berlin Heidelberg 2011

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains a collection of studies in the areas of complexity theory and foundations of cryptography. These studies were conducted at different times during the last couple of decades. Although many of these studies have been referred to by other works, none of them was formally published before.

Indeed, this volume is quite unusual, and it raises two opposite questions regarding the publication of the foregoing studies: (1) why were these studies not published (formally) before, and (2) why are they being published now?

Let me start with the second question. In the years that have elapsed since the completion of many of these individual studies, I have occasionally looked at them for some reason. On these occasions, I felt that it is somewhat inappropriate that these works were never published formally (although many of them were posted on forums such as ECCC). The current volume is aimed at amending this situation somewhat.

Turning to the first question, the answer varies according to the case. Regarding the surveys and the programmatic and/or reflective articles, the answer is quite straightforward: The standard publication venues for research in complexity and/or cryptography do not welcome such articles, which may reflect the unfortunate fact that our community does not hold such articles in high esteem. Regarding the articles that describe research contributions, the answer varies from the non-existence of an adequate venue (at least at the relevant time), to unjustified (in retrospect) timidity regarding the work.

The late publication of some of these articles also raises questions regarding the relation of the current versions to the original ones. These questions are addressed at the beginning of each individual article, where the original posting is stated and the nature of the revision is outlined. In general, all articles were revised (based on their last posted version), but the revision attempts to preserve the spirit of the original work. In the few cases that later developments suggest a different perspective and/or technical improvements, this is stated explicitly while comparing the original perspective and/or results with the current one.

The compilation of this volume led me to complete the writing of a couple of surveys. In addition, I decided to also include in this volume a few rather recent research contributions.

The studies in this volume are arranged in three parts. Part I contains 20 research contributions, Part II contain 12 surveys (and one overview essay on “Randomness and Computation”), and Part III contains three programmatic and/or reflective articles. Most studies in Part I (and a couple of the studies in Part II) were conducted by me in collaboration with other researchers.

The topics addressed in the various studies 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 (PCPs), proofs of knowledge, property testing, pseudorandomness, randomness extractors, sampling, trapdoor permutations, zero-knowledge and non-interactive zero-knowledge (NIZK). Indeed, one may say that most of these works belong to the interplay between randomness and computation.

Part I: Research Contributions

1. The Shortest Move-Sequence in the Generalized 15-Puzzle Is NP-Hard
2. Proofs of Computational Ability
3. On Constructing 1-1 One-way Functions
4. On the Circuit Complexity of Perfect Hashing
5. Collision-Free Hashing from Lattice Problems
6. Another Proof that BPP Is Contained in PH (and More)
7. Strong Proofs of Knowledge
8. Simplified Derandomization of BPP Using a Hitting Set Generator
9. On Testing Expansion in Bounded-Degree Graphs
10. A Candidate One-Way Functions Based on Expander Graphs
11. The FGLSS-Reduction and Minimum Vertex Cover in Hypergraphs
12. The GGM Construction Does NOT Yield Correlation Intractability
13. On Logarithmic Versus Single-Bit Advice
14. On Proofs Of Knowledge: Probabilistic Versus Deterministic Provers
15. On the Average-Case Complexity of Property Testing
16. A Candidate Counterexample to the Easy Cylinders Conjecture
17. From Absolute Distinguishability to Positive Distinguishability
18. Testing Graph Blow-Up
19. Proximity Oblivious Testing and the Role of Invariances
20. In a World of $P=BPP$

Part II: Surveys

1. On Levin's Theory of Average-Case Complexity
2. On Three XOR-Lemmas
3. On Yao's XOR-Lemma
4. A Sample of Samplers – A Computational Perspective on Sampling
5. Short Locally Testable Codes and Proofs
6. Bravely, Moderately: A Common Theme in Four Recent Results
7. On the Complexity of Computational Problems Regarding Distributions
8. On Basing Non-Interactive Zero-Knowledge on Trapdoor Permutations
9. Average Case Complexity, Revisited
10. Basic Facts About Expander Graphs
11. A Brief Introduction to Property Testing
12. Introduction to Testing Graph Properties

Part III: Programmatic and Reflective Articles

1. On Security Preserving Reductions – A Suggested Terminology
2. Contemplations on Testing Graph Properties
3. Another Motivation for Reducing the Randomness Complexity of Algorithms

I am grateful to all of my co-authors of the papers included in the current volume: Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, and David Zuckerman. In addition, I wish to thank all researchers who have contributed to the research being surveyed in this volume.

Oded Goldreich

Table of Contents

Research Contributions

Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle Is NP-Hard	1
<i>Oded Goldreich</i>	
Proving Computational Ability	6
<i>Mihir Bellare and Oded Goldreich</i>	
On Constructing 1-1 One-Way Functions.....	13
<i>Oded Goldreich, Leonid A. Levin, and Noam Nisan</i>	
On the Circuit Complexity of Perfect Hashing	26
<i>Oded Goldreich and Avi Wigderson</i>	
Collision-Free Hashing from Lattice Problems	30
<i>Oded Goldreich, Shafi Goldwasser, and Shai Halevi</i>	
Another Proof That $\mathcal{BPP} \subseteq \mathcal{PH}$ (and More)	40
<i>Oded Goldreich and David Zuckerman</i>	
Strong Proofs of Knowledge	54
<i>Oded Goldreich</i>	
Simplified Derandomization of BPP Using a Hitting Set Generator	59
<i>Oded Goldreich, Salil Vadhan, and Avi Wigderson</i>	
On Testing Expansion in Bounded-Degree Graphs.....	68
<i>Oded Goldreich and Dana Ron</i>	
Candidate One-Way Functions Based on Expander Graphs	76
<i>Oded Goldreich</i>	
Using the FGLSS-Reduction to Prove Inapproximability Results for Minimum Vertex Cover in Hypergraphs	88
<i>Oded Goldreich</i>	
The GGM Construction Does NOT Yield Correlation Intractable Function Ensembles	98
<i>Oded Goldreich</i>	
From Logarithmic Advice to Single-Bit Advice.....	109
<i>Oded Goldreich, Madhu Sudan, and Luca Trevisan</i>	

On Probabilistic versus Deterministic Provers in the Definition of Proofs of Knowledge	114
<i>Mihir Bellare and Oded Goldreich</i>	
On the Average-Case Complexity of Property Testing	124
<i>Oded Goldreich</i>	
A Candidate Counterexample to the Easy Cylinders Conjecture.....	136
<i>Oded Goldreich</i>	
From Absolute Distinguishability to Positive Distinguishability	141
<i>Zvika Brakerski and Oded Goldreich</i>	
Testing Graph Blow-Up.....	156
<i>Lidor Avigad and Oded Goldreich</i>	
Proximity Oblivious Testing and the Role of Invariances	173
<i>Oded Goldreich and Tali Kaufman</i>	
In a World of $P=BPP$	191
<i>Oded Goldreich</i>	
Surveys	
Notes on Levin's Theory of Average-Case Complexity	233
<i>Oded Goldreich</i>	
Three XOR-Lemmas — An Exposition	248
<i>Oded Goldreich</i>	
On Yao's XOR-Lemma	273
<i>Oded Goldreich, Noam Nisan, and Avi Wigderson</i>	
A Sample of Samplers: A Computational Perspective on Sampling	302
<i>Oded Goldreich</i>	
Short Locally Testable Codes and Proofs.....	333
<i>Oded Goldreich</i>	
Bravely, Moderately: A Common Theme in Four Recent Works	373
<i>Oded Goldreich</i>	
On the Complexity of Computational Problems Regarding Distributions	390
<i>Oded Goldreich and Salil Vadhan</i>	
Basing Non-Interactive Zero-Knowledge on (Enhanced) Trapdoor Permutations: The State of the Art	406
<i>Oded Goldreich</i>	

Average Case Complexity, Revisited	422
<i>Oded Goldreich</i>	
Basic Facts about Expander Graphs	451
<i>Oded Goldreich</i>	
A Brief Introduction to Property Testing	465
<i>Oded Goldreich</i>	
Introduction to Testing Graph Properties	470
<i>Oded Goldreich</i>	
Randomness and Computation	507
<i>Oded Goldreich</i>	
 Programmatic and Reflective Articles	
On Security Preserving Reductions – Revised Terminology	540
<i>Oded Goldreich</i>	
Contemplations on Testing Graph Properties	547
<i>Oded Goldreich</i>	
Another Motivation for Reducing the Randomness Complexity of Algorithms	555
<i>Oded Goldreich</i>	
About the Authors	561