Lecture Notes in Computer Science 6650

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

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) timidness 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 "Randombess 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-interative zero-knowledge (NIZK). Indeed, one may say that most of these works belong to the interplay between randomness and computation.

Part I: Research Contributions

Part II: Surveys

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

Surveys

Programmatic and Reflective Articles