



Algorithms and Combinatorics 17

Editorial Board

R.L. Graham, Murray Hill B. Korte, Bonn

L. Lovász, Budapest A. Wigderson, Jerusalem

G.M. Ziegler, Berlin

Oded Goldreich

Modern Cryptography,
Probabilistic Proofs
and Pseudorandomness



Springer

Oded Goldreich
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
76100 Rehovot
Israel
e-mail: oded@wisdom.weizmann.ac.il

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Goldreich, Oded: Modern cryptography, probabilistic proofs and pseudorandomness / Oded Goldreich.

(Algorithms and combinatorics; 17)

ISBN 978-3-642-08432-4 ISBN 978-3-662-12521-2 (eBook)

DOI 10.1007/978-3-662-12521-2

Mathematics Subject Classification (1991): 68-02, 68-Q, 68-R,
03-B99, 60-A99, 90-D99

ISSN 0937-5511

ISBN 978-3-642-08432-4

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, reuse 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-Verlag Berlin Heidelberg GmbH.

Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1999

Originally published by Springer-Verlag Berlin Heidelberg New York in 1999

Softcover reprint of the hardcover 1st edition 1999

Typesetting: Typeset in LaTeX by the author. Reformatted by Kurt Mattes, Heidelberg, using a Springer TeX macro package

SPIN 10675255 46/3143 - 5 4 3 2 1 0 - Printed on acid-free paper

To Dana

Preface

You can start by putting the DO NOT DISTURB sign.

Cay, in *Desert Hearts* (1985).

The interplay between randomness and computation is one of the most fascinating scientific phenomena uncovered in the last couple of decades. This interplay is at the heart of modern cryptography and plays a fundamental role in complexity theory at large. Specifically, the interplay of randomness and computation is pivotal to several intriguing notions of probabilistic proof systems and is the focal of the computational approach to randomness. This book provides an introduction to these three, somewhat interwoven domains (i.e., cryptography, proofs and randomness).

Modern Cryptography. Whereas classical cryptography was confined to the art of designing and breaking encryption schemes (or “secrecy codes”), Modern Cryptography is concerned with the rigorous analysis of any system which should withstand malicious attempts to abuse it. We emphasize two aspects of the transition from classical to modern cryptography: (1) the widening of scope from one specific task to an utmost wide general class of tasks; and (2) the move from an engineering-art which strives on ad-hoc tricks to a scientific discipline based on rigorous approaches and techniques.

In this book we provide an introduction to the foundations of Modern Cryptography. We focus on the paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural cryptographic problems. We also survey some of the fundamental results obtained using these paradigms, approaches and techniques. The emphasis of the exposition is on the need for and impact of a rigorous approach.

Probabilistic Proof Systems. Various types of *probabilistic* proof systems have played a central role in the development of computer science in the last decade. These proof systems share a common (untraditional) feature – they carry a probability of error; yet, this probability is explicitly bounded and can be reduced by successive application of the proof system. The gain in allowing this untraditional relaxation is substantial, as demonstrated by three well known results regarding *interactive proofs*, *zero-knowledge proofs*,

and *probabilistic checkable proofs*: In each of these cases, allowing a bounded probability of error makes the system much more powerful and useful than the traditional (errorless) counterparts.

Focusing on the three types of proof systems mentioned above, but going also beyond them, we survey the basic definitions and results regarding probabilistic proofs. Our exposition stresses both the similarities and differences between the various types of probabilistic proofs.

Pseudorandomness. A fresh view at the *question of randomness* was taken in the theory of computing: It has been postulated that a distribution is pseudorandom if it cannot be told apart from the uniform distribution by any efficient procedure. This paradigm, originally associating efficient procedures with polynomial-time algorithms, has been applied also with respect to a variety of limited classes of such distinguishing procedures.

Starting with the general paradigm, we survey the archetypical case of pseudorandom generators (withstanding any polynomial-time distinguisher), as well as generators withstanding space-bounded distinguishers, the derandomization of complexity classes such as \mathcal{BPP} , and some special-purpose generators.

An Underlying Assumption

Much of the contents of this book depends on the widely believed conjecture by which $\mathcal{P} \neq \mathcal{NP}$. This dependency is explicitly stated in some of the results which make even stronger assumptions (such as the existence of one-way functions), and is implicit in some results (such as the PCP Characterization of NP) which would become uninteresting if $\mathcal{P} = \mathcal{NP}$.

On the Nature of this Book

This book offers an introduction and extensive survey to each of the three areas mentioned above. It present both the basic notions and the most important (and sometimes advanced) results. The presentation is focused on the essentials and does not elaborate on details. In some cases it offers a novel and illuminating perspective. The goal is to provide the reader with

1. A clear and structured overview of each of these areas.
2. Knowledge of the most important notions, ideas, techniques and results in each area.
3. Some new insights into each of these areas.

It is hoped that the book may be useful both to a beginner (who has only some background in the theory of computing), and to an expert in any of these areas.

Organization

In Chapter 1 we survey the basic concepts, definitions and results in cryptography. In particular, we survey the basic tools of cryptography – computational difficulty, pseudorandomness and zero-knowledge proofs – and the basic utilities – encryption, signatures, and general cryptographic protocols. Chapters 2 and 3 provides a wider perspective on two concepts mentioned in Chapter 1. Specifically, Chapter 2 surveys various types of probabilistic proof systems including interactive proofs, zero-knowledge proofs and probabilistically checkable proofs (PCP). (The overlap with Chapter 1 is small, and the presentation is quite different.) Likewise, Chapter 3 surveys various notions of pseudorandom generators, viewing the one discussed in Chapter 1 as an archetypical instantiation of a general paradigm.

The three chapters may be read independently of each other. In particular, each starts with an individual brief introduction to the respective subject matter. As hinted above, although the chapters do overlap, the perspectives taken in them are different. Specifically, Chapter 1 treats the theoretical foundations of a practical discipline, and so the presentation departs from practice and emphasizes *the importance of rigorous treatment for sound practice* (and not merely *per se*). In contrast, Chapters 2 and 3 depart from the theory of computing and emphasize the intellectual contents of the material (rather than its practical applicability). The fact that different perspectives co-exist in the same book, let alone in the same author, is indicative of the nature of the theory of computing.

The three chapters are augmented by four appendices and an extensive bibliography. Most importantly, Appendix A provides some basic background on computation and randomness.

We mention that important relations between randomness and computation were discovered also in other domains of the theory of computation. Some examples are given in Appendix B.

Appendix C provides proofs of two basic results; one being a folklore for which no proof has ever appeared, and the other for which the published proof is both too terse and more complex than the alternative presented here.

Acknowledgments

Much of the material was written while visiting the Laboratory for Computer Science of MIT.

A preliminary version of Chapter 1 has appeared in the proceedings of *Advances in Cryptology – Crypto97*, Springer’s Lecture Notes in Computer Science (1997), Vol. 1294, pages 46–74.

Parts of the material presented in Chapter 2 have appeared in the proceedings of *STACS97*, Springer’s Lecture Notes in Computer Science (1997), Vol. 1200, pages 595–611.

As for personal acknowledgments, I will only mention some of the people to whom I am most indebted for my professional development. These include Benny Chor, Shimon Even, Shafi Goldwasser, Leonid Levin, Silvio Micali, and Avi Wigderson.

.... very little do we have and inclose which we can call our own in the deep sense of the word. We all have to accept and learn, either from our predecessors or from our contemporaries. Even the greatest genius would not have achieved much if he had wished to extract everything from inside himself. But there are many good people, who do not understand this, and spend half their lives wondering in darkness with their dreams of originality. I have known artists who were proud of not having followed any teacher and of owing everything only to their own genius. Such fools!

[Goethe, *Conversations with Eckermann*, 17.2.1832]

Table of Contents

1. The Foundations of Modern Cryptography	1
1.1 Introduction	1
1.2 Central Paradigms	5
1.2.1 Computational Difficulty	7
1.2.2 Computational Indistinguishability	8
1.2.3 The Simulation Paradigm	8
1.3 Pseudorandomness	9
1.3.1 The Basics	9
1.3.2 Pseudorandom Functions	10
1.4 Zero-Knowledge	12
1.4.1 The Basics	12
1.4.2 Some Variants	13
1.5 Encryption	15
1.5.1 Definitions	15
1.5.2 Constructions	17
1.5.3 Security Beyond Passive Attacks	19
1.6 Signatures	20
1.6.1 Definitions	21
1.6.2 Constructions	21
1.6.3 Two Variants	23
1.7 Cryptographic Protocols	24
1.7.1 Definitions	25
1.7.2 Constructions	26
1.8 Some Notes	26
1.8.1 General Notes	27
1.8.2 Specific Notes	31
1.9 Historical Perspective	33
1.10 Two Suggestions for Future Research	35
1.11 Some Suggestions for Further Reading	36
2. Probabilistic Proof Systems	39
2.1 Introduction	39
2.2 Interactive Proof Systems	41
2.2.1 Definition	41

2.2.2	The Role of Randomness	42
2.2.3	The Power of Interactive Proofs	43
2.2.4	The Interactive Proof System Hierarchy	47
2.2.5	How Powerful Should the Prover Be?	48
2.3	Zero-Knowledge Proof Systems	49
2.3.1	A Sample Definition	49
2.3.2	The Power of Zero-Knowledge	51
2.3.3	The Role of Randomness	53
2.4	Probabilistically Checkable Proof Systems	53
2.4.1	Definition	53
2.4.2	The Power of Probabilistically Checkable Proofs	54
2.4.3	PCP and Approximation	57
2.4.4	More on PCP Itself	58
2.4.5	The Role of Randomness	60
2.5	Other Probabilistic Proof Systems	61
2.5.1	Restricting the Prover's Strategy	61
2.5.2	Non-Interactive Proofs	64
2.5.3	Proofs of Knowledge	64
2.5.4	Refereed Games	65
2.6	Concluding Remarks	65
2.6.1	Comparison Among the Various Notions	65
2.6.2	The Story	67
2.6.3	Open Problems	71
3.	Pseudorandom Generators	73
3.1	Introduction	73
3.2	The General Paradigm	75
3.3	The Archetypical Case	77
3.3.1	A Short Discussion	78
3.3.2	Some Basic Observations	79
3.3.3	Constructions	82
3.3.4	Pseudorandom Functions	85
3.4	Derandomization of Time-complexity Classes	87
3.5	Space Pseudorandom Generators	88
3.6	Special Purpose Generators	92
3.6.1	Pairwise-Independence Generators	93
3.6.2	Small-Bias Generators	95
3.6.3	Random Walks on Expanders	96
3.6.4	Samplers	98
3.6.5	Dispersers, Extractors and Weak Random Sources	101
3.7	Concluding Remarks	103
3.7.1	Discussion	104
3.7.2	Historical Perspective	104
3.7.3	Open Problems	106

A. Background on Randomness and Computation	107
A.1 Probability Theory – Three Inequalities	107
A.2 Computational Models and Complexity Classes	110
A.2.1 P, NP, and More	110
A.2.2 Probabilistic Polynomial-Time	111
A.2.3 Non-Uniform Polynomial-Time	113
A.2.4 Oracle Machines	115
A.2.5 Space Bounded Machines	116
A.2.6 Average-Case Complexity	117
A.3 Complexity Classes – Glossary	118
A.4 Some Basic Cryptographic Settings	119
A.4.1 Encryption Schemes	119
A.4.2 Digital Signatures and Message Authentication	121
A.4.3 The RSA and Rabin Functions	123
B. Randomized Computations	125
B.1 Randomized Algorithms	125
B.1.1 Approx. Counting of DNF Satisfying Assignments	126
B.1.2 Finding a Perfect Matching	127
B.1.3 Testing Whether Polynomials Are Identical	130
B.1.4 Randomized Rounding Applied to MaxSAT	131
B.1.5 Primality Testing	132
B.1.6 Testing Graph Connectivity via a Random Walk	133
B.1.7 Finding Minimum Cuts in Graphs	134
B.2 Randomness in Complexity Theory	135
B.2.1 Reducing (Approximate) Counting to Deciding	135
B.2.2 Two-sided Error Versus One-sided Error	137
B.2.3 The Permanent: Worst-Case vs Average Case	138
B.3 Randomness in Distributed Computing	139
B.3.1 Testing String Equality	139
B.3.2 Routing in Networks	140
B.3.3 Byzantine Agreement	141
B.4 Bibliographic Notes	143
C. Two Proofs	145
C.1 Parallel Repetition of Interactive Proofs	145
C.2 A Generic Hard-Core Predicate	149
C.2.1 A Motivating Discussion	151
C.2.2 Back to the Formal Argument	152
C.2.3 Improved Implementation of Algorithm A'	154
D. Related Surveys by the Author	157
Bibliography	159
Index	179