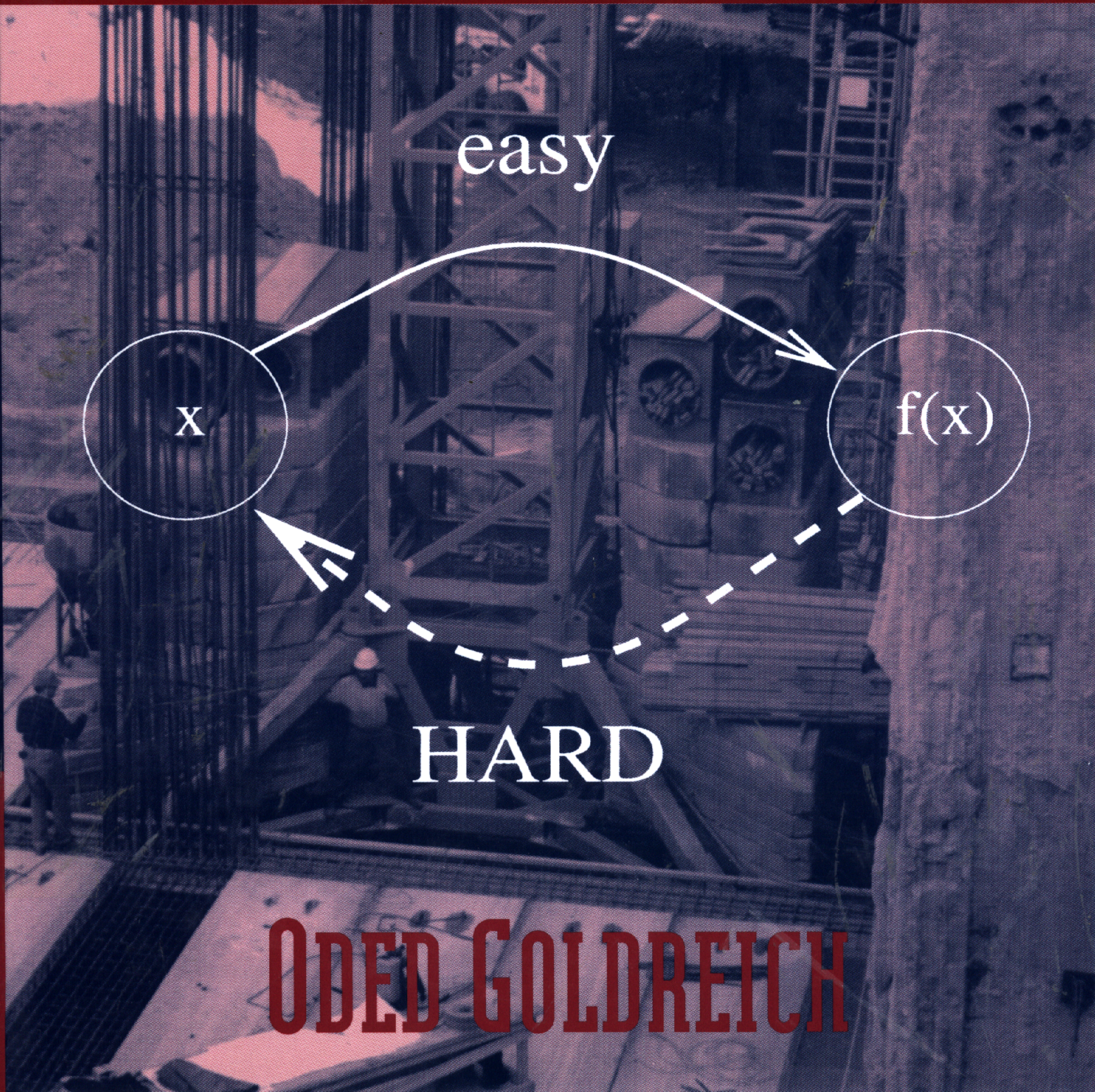
FOUNDATIONS OF CRYPTOGRAPHY

Volume I Basic Tools



ODED GOLDREICH

BIBLIOTHEQUE DU CERIST

IST 2904

Foundations of Cryptography

Volume I Basic Tools

Oded Goldreich

Weizmann Institute of Science

BIBLIOTHEQUE DU CERIST

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

© Oded Goldreich 2001

This book is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2001
Reprinted with corrections 2003

Printed in the United States of America

Typefaces Times Roman 10.5/13 pt. and Helvetica *System* LaTeX 2_ε [TB]

A catalog record for this book is available from the British Library.

Library of Congress Cataloging in Publication data
Goldreich, Oded.
Foundations of cryptography : basic tools / Oded Goldreich.
p. cm.
Includes bibliographical references and index.
ISBN 0-521-79172-3
1. Coding theory. 2. Cryptography – Mathematics. I. Title.
QA268.G5745 2001
652′.8 – dc21 00-049362

ISBN 0 521 79172 3 hardback

BIBLIOTHEQUE DU CERIST

7823

BIBLIOTHEQUE DU CERIST

Foundations of Cryptography

Cryptography is concerned with the conceptualization, definition, and construction of computing systems that address security concerns. The design of cryptographic systems must be based on firm foundations. This book presents a rigorous and systematic treatment of the foundational issues: defining cryptographic tasks and solving new cryptographic problems using existing tools. It focuses on the basic mathematical tools: computational difficulty (one-way functions), pseudorandomness, and zero-knowledge proofs. The emphasis is on the clarification of fundamental concepts and on demonstrating the feasibility of solving cryptographic problems rather than on describing ad hoc approaches.

The book is suitable for use in a graduate course on cryptography and as a reference book for experts. The author assumes basic familiarity with the design and analysis of algorithms; some knowledge of complexity theory and probability is also useful.

Oded Goldreich is Professor of Computer Science at the Weizmann Institute of Science and incumbent of the Meyer W. Weisgal Professorial Chair. An active researcher, he has written numerous papers on cryptography and is widely considered to be one of the world experts in the area. He is an editor of *Journal of Cryptology* and *SIAM Journal on Computing* and the author of *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, published in 1999 by Springer-Verlag.

BIBLIOTHEQUE DU CERIST

Contents

BIBLIOTHEQUE DU CERIST

List of Figures *page* xii
Preface xiii

1 Introduction **1**

1.1. Cryptography: Main Topics 1
1.1.1. Encryption Schemes 2
1.1.2. Pseudorandom Generators 3
1.1.3. Digital Signatures 4
1.1.4. Fault-Tolerant Protocols and Zero-Knowledge Proofs 6
1.2. Some Background from Probability Theory 8
1.2.1. Notational Conventions 8
1.2.2. Three Inequalities 9
1.3. The Computational Model 12
1.3.1. $\mathcal{P}$, $\mathcal{NP}$, and $\mathcal{NP}$-Completeness 12
1.3.2. Probabilistic Polynomial Time 13
1.3.3. Non-Uniform Polynomial Time 16
1.3.4. Intractability Assumptions 19
1.3.5. Oracle Machines 20
1.4. Motivation to the Rigorous Treatment 21
1.4.1. The Need for a Rigorous Treatment 21
1.4.2. Practical Consequences of the Rigorous Treatment 23
1.4.3. The Tendency to Be Conservative 24
1.5. Miscellaneous 25
1.5.1. Historical Notes 25
1.5.2. Suggestions for Further Reading 27
1.5.3. Open Problems 27
1.5.4. Exercises 28

BIBLIOTHEQUE DU CERIST

2 Computational Difficulty **30**

2.1. One-Way Functions: Motivation 31
2.2. One-Way Functions: Definitions 32
2.2.1. Strong One-Way Functions 32
2.2.2. Weak One-Way Functions 35
2.2.3. Two Useful Length Conventions 35
2.2.4. Candidates for One-Way Functions 40
2.2.5. Non-Uniformly One-Way Functions 41
2.3 Weak One-Way Functions Imply Strong Ones 43
2.3.1. The Construction and Its Analysis (Proof of Theorem 2.3.2) 44
2.3.2. Illustration by a Toy Example 48
2.3.3. Discussion 50
2.4. One-Way Functions: Variations 51
2.4.1.* Universal One-Way Function 52
2.4.2. One-Way Functions as Collections 53
2.4.3. Examples of One-Way Collections 55
2.4.4. Trapdoor One-Way Permutations 58
2.4.5.* Claw-Free Functions 60
2.4.6.* On Proposing Candidates 63
2.5. Hard-Core Predicates 64
2.5.1. Definition 64
2.5.2. Hard-Core Predicates for Any One-Way Function 65
2.5.3.* Hard-Core Functions 74
2.6.* Efficient Amplification of One-Way Functions 78
2.6.1. The Construction 80
2.6.2. Analysis 81
2.7. Miscellaneous 88
2.7.1. Historical Notes 89
2.7.2. Suggestions for Further Reading 89
2.7.3. Open Problems 91
2.7.4. Exercises 92

3 Pseudorandom Generators **101**

3.1. Motivating Discussion 102
3.1.1. Computational Approaches to Randomness 102
3.1.2. A Rigorous Approach to Pseudorandom Generators 103
3.2. Computational Indistinguishability 103
3.2.1. Definition 104
3.2.2. Relation to Statistical Closeness 106
3.2.3. Indistinguishability by Repeated Experiments 107
3.2.4.* Indistinguishability by Circuits 111
3.2.5. Pseudorandom Ensembles 112
3.3. Definitions of Pseudorandom Generators 112
3.3.1. Standard Definition of Pseudorandom Generators 113

3.3.2. Increasing the Expansion Factor 114
3.3.3.* Variable-Output Pseudorandom Generators 118
3.3.4. The Applicability of Pseudorandom Generators 119
3.3.5. Pseudorandomness and Unpredictability 119
3.3.6. Pseudorandom Generators Imply One-Way Functions 123
3.4. Constructions Based on One-Way Permutations 124
3.4.1. Construction Based on a Single Permutation 124
3.4.2. Construction Based on Collections of Permutations 131
3.4.3.* Using Hard-Core Functions Rather than Predicates 134
3.5.* Constructions Based on One-Way Functions 135
3.5.1. Using 1-1 One-Way Functions 135
3.5.2. Using Regular One-Way Functions 141
3.5.3. Going Beyond Regular One-Way Functions 147
3.6. Pseudorandom Functions 148
3.6.1. Definitions 148
3.6.2. Construction 150
3.6.3. Applications: A General Methodology 157
3.6.4.* Generalizations 158
3.7.* Pseudorandom Permutations 164
3.7.1. Definitions 164
3.7.2. Construction 166
3.8. Miscellaneous 169
3.8.1. Historical Notes 169
3.8.2. Suggestions for Further Reading 170
3.8.3. Open Problems 172
3.8.4. Exercises 172

4 Zero-Knowledge Proof Systems 184

4.1. Zero-Knowledge Proofs: Motivation 185
4.1.1. The Notion of a Proof 187
4.1.2. Gaining Knowledge 189
4.2. Interactive Proof Systems 190
4.2.1. Definition 190
4.2.2. An Example (Graph Non-Isomorphism in $\mathcal{IP}$) 195
4.2.3.* The Structure of the Class $\mathcal{IP}$ 198
4.2.4. Augmentation of the Model 199
4.3. Zero-Knowledge Proofs: Definitions 200
4.3.1. Perfect and Computational Zero-Knowledge 200
4.3.2. An Example (Graph Isomorphism in $\mathcal{PZK}$) 207
4.3.3. Zero-Knowledge with Respect to Auxiliary Inputs 213
4.3.4. Sequential Composition of Zero-Knowledge Proofs 216
4.4. Zero-Knowledge Proofs for $\mathcal{NP}$ 223
4.4.1. Commitment Schemes 223
4.4.2. Zero-Knowledge Proof of Graph Coloring 228

BIBLIOTHEQUE DU CERIST

4.4.3. The General Result and Some Applications 240
4.4.4. Second-Level Considerations 243
4.5.* Negative Results 246
4.5.1. On the Importance of Interaction and Randomness 247
4.5.2. Limitations of Unconditional Results 248
4.5.3. Limitations of Statistical ZK Proofs 250
4.5.4. Zero-Knowledge and Parallel Composition 251
4.6.* Witness Indistinguishability and Hiding 254
4.6.1. Definitions 254
4.6.2. Parallel Composition 258
4.6.3. Constructions 259
4.6.4. Applications 261
4.7.* Proofs of Knowledge 262
4.7.1. Definition 262
4.7.2. Reducing the Knowledge Error 267
4.7.3. Zero-Knowledge Proofs of Knowledge for $\mathcal{NP}$ 268
4.7.4. Applications 269
4.7.5. Proofs of Identity (Identification Schemes) 270
4.7.6. Strong Proofs of Knowledge 274
4.8.* Computationally Sound Proofs (Arguments) 277
4.8.1. Definition 277
4.8.2. Perfectly Hiding Commitment Schemes 278
4.8.3. Perfect Zero-Knowledge Arguments for $\mathcal{NP}$ 284
4.8.4. Arguments of Poly-Logarithmic Efficiency 286
4.9.* Constant-Round Zero-Knowledge Proofs 288
4.9.1. Using Commitment Schemes with Perfect Secrecy 289
4.9.2. Bounding the Power of Cheating Provers 294
4.10.* Non-Interactive Zero-Knowledge Proofs 298
4.10.1. Basic Definitions 299
4.10.2. Constructions 300
4.10.3. Extensions 306
4.11.* Multi-Prover Zero-Knowledge Proofs 311
4.11.1. Definitions 311
4.11.2. Two-Sender Commitment Schemes 313
4.11.3. Perfect Zero-Knowledge for $\mathcal{NP}$ 317
4.11.4. Applications 319
4.12. Miscellaneous 320
4.12.1. Historical Notes 320
4.12.2. Suggestions for Further Reading 322
4.12.3. Open Problems 323
4.12.4. Exercises 323
Appendix A: Background in Computational Number Theory **331**
A.1. Prime Numbers 331
A.1.1. Quadratic Residues Modulo a Prime 331

BIBLIOTHEQUE DU CERIST

A.1.2. Extracting Square Roots Modulo a Prime 332
A.1.3. Primality Testers 332
A.1.4. On Uniform Selection of Primes 333
A.2. Composite Numbers 334
A.2.1. Quadratic Residues Modulo a Composite 335
A.2.2. Extracting Square Roots Modulo a Composite 335
A.2.3. The Legendre and Jacobi Symbols 336
A.2.4. Blum Integers and Their Quadratic-Residue Structure 337

Appendix B: Brief Outline of Volume 2 338

B.1. Encryption: Brief Summary 338
B.1.1. Definitions 338
B.1.2. Constructions 340
B.1.3. Beyond Eavesdropping Security 343
B.1.4. Some Suggestions 345
B.2. Signatures: Brief Summary 345
B.2.1. Definitions 346
B.2.2. Constructions 347
B.2.3. Some Suggestions 349
B.3. Cryptographic Protocols: Brief Summary 350
B.3.1. Definitions 350
B.3.2. Constructions 352
B.3.3. Some Suggestions 353

Bibliography 355
Index 367

Note: Asterisks throughout Contents indicate advanced material.

BIBLIOTHEQUE DU CERIST