Contents

1 Introduction 11

1.1 Cryptography – Main Topics 11
  1.1.1 Encryption Schemes 11
  1.1.2 Pseudorandom Generators 13
  1.1.3 Digital Signatures 14
  1.1.4 Fault-Tolerant Protocols and Zero-Knowledge Proofs 16
1.2 Some Background from Probability Theory 18
  1.2.1 Notational Conventions 18
  1.2.2 Three Inequalities 19
1.3 The Computational Model 23
  1.3.1 P, NP, and NP-completeness 23
  1.3.2 Probabilistic Polynomial-Time 24
  1.3.3 Non-Uniform Polynomial-Time 27
  1.3.4 Intractability Assumptions 29
  1.3.5 Oracle Machines 30
1.4 Motivation to the Formal Treatment 31
  1.4.1 The Need to Formalize Intuition 31
  1.4.2 The Practical Consequences of the Formal Treatment 32
  1.4.3 The Tendency to be Conservative 33

2 Computational Difficulty 35

2.1 One-Way Functions: Motivation 35

2.2 One-Way Functions: Definitions 36

2.2.1 Strong One-Way Functions 36

2.2.2 Weak One-Way Functions 38

2.2.3 Two Useful Length Conventions 39

2.2.4 Candidates for One-Way Functions 42

2.2.5 Non-Uniformly One-Way Functions 44

2.3 Weak One-Way Functions Imply Strong Ones 45

2.4 One-Way Functions: Variations 51

2.4.1 * Universal One-Way Function 51

2.4.2 One-Way Functions as Collections 52

2.4.3 Examples of One-way Collections (RSA, Factoring, DLP) 54

2.4.4 Trapdoor one-way permutations 57

2.4.5 * Clawfree Functions 58

2.4.6 On Proposing Candidates 61

2.5 Hard-Core Predicates 61

2.5.1 Definition 62

2.5.2 Hard-Core Predicates for any One-Way Function 63

2.5.3 * Hard-Core Functions 67

2.6 * Efficient Amplification of One-way Functions 70

2.7 Miscellaneous 76

2.7.1 Historical Notes 76

2.7.2 Suggestion for Further Reading 77

2.7.3 Open Problems 78

2.7.4 Exercises 78

3 Pseudorandom Generators 85

3.1 Motivating Discussion 85
3.1.1 Computational Approaches to Randomness 85
3.1.2 A Rigorous Approach to Pseudorandom Generators 86
3.2 Computational Indistinguishability 87
3.2.1 Definition 87
3.2.2 Relation to Statistical Closeness 89
3.2.3 Indistinguishability by Repeated Experiments 90
3.2.4 Pseudorandom Ensembles 94
3.3 Definitions of Pseudorandom Generators 94
3.3.1 * A General Definition of Pseudorandom Generators 95
3.3.2 Standard Definition of Pseudorandom Generators 96
3.3.3 Increasing the Expansion Factor of Pseudorandom Generators . . . 96
3.3.4 The Significance of Pseudorandom Generators 100
3.3.5 A Necessary Condition for the Existence of Pseudorandom Generators 101
3.4 Constructions based on One-Way Permutations 102
3.4.1 Construction based on a Single Permutation 102
3.4.2 Construction based on Collections of Permutations 104
3.4.3 Practical Constructions 106
3.5 * Construction based on One-Way Functions 106
3.5.1 Using 1-1 One-Way Functions 106
3.5.2 Using Regular One-Way Functions 112
3.5.3 Going beyond Regular One-Way Functions 117
3.6 Pseudorandom Functions 118
3.6.1 Definitions 118
3.6.2 Construction 120
3.7 * Pseudorandom Permutations 125
3.7.1 Definitions 125
3.7.2 Construction 127

3.8 Miscellaneous 130
3.8.1 Historical Notes 130
3.8.2 Suggestion for Further Reading 131
3.8.3 Open Problems 132
3.8.4 Exercises 132

4 Encryption Schemes 139

5 Digital Signatures and Message Authentication 141

6 Zero-Knowledge Proof Systems 143
6.1 Zero-Knowledge Proofs: Motivation 143
6.1.1 The Notion of a Proof 144
6.1.2 Gaining Knowledge 146
6.2 Interactive Proof Systems 148
6.2.1 Definition 148
6.2.2 An Example (Graph Non-Isomorphism in IP) 153
6.2.3 Augmentation to the Model 156
6.3 Zero-Knowledge Proofs: Definitions 157
6.3.1 Perfect and Computational Zero-Knowledge 157
6.3.2 An Example (Graph Isomorphism in PZK) 162
6.3.3 Zero-Knowledge w.r.t. Auxiliary Inputs 167
6.3.4 Sequential Composition of Zero-Knowledge Proofs 169
6.4 Zero-Knowledge Proofs for NP 175
6.4.1 Commitment Schemes 175
6.4.2 Zero-Knowledge proof of Graph Coloring 180
6.4.3 The General Result and Some Applications 191
6.4.4 Efficiency Considerations 194
6.5 * Negative Results 196
6.5.1 Implausibility of an Unconditional “NP in ZK” Result 197
6.5.2 Implausibility of Perfect Zero-Knowledge proofs for all of NP 198

6.5.3 Zero-Knowledge and Parallel Composition 199
6.6 * Witness Indistinguishability and Hiding 202
6.6.1 Definitions 202
6.6.2 Parallel Composition 205
6.6.3 Constructions 206
6.6.4 Applications 208
6.7 * Proofs of Knowledge 208
6.7.1 Definition 209
6.7.2 Observations 211
6.7.3 Applications 212
6.7.4 Proofs of Identity (Identification schemes) 213
6.8 * Computationally-Sound Proofs (Arguments) 217
6.8.1 Definition 218
6.8.2 Perfect Commitment Schemes 219
6.8.3 Perfect Zero-Knowledge Arguments for NP 225
6.8.4 Zero-Knowledge Arguments of Polylogarithmic Efficiency 227
6.9 * Constant Round Zero-Knowledge Proofs 228
6.9.1 Using commitment schemes with perfect secrecy 230
6.9.2 Bounding the power of cheating provers 234
6.10 * Non-Interactive Zero-Knowledge Proofs 237
6.10.1 Definition 237
6.10.2 Construction 237
6.11 * Multi-Prover Zero-Knowledge Proofs 237
6.11.1 Definitions 238
6.11.2 Two-Senders Commitment Schemes 240
6.11.3 Perfect Zero-Knowledge for NP 244
6.11.4 Applications 246
6.12 Miscellaneous 247
6.12.1 Historical Notes 247
6.12.2 Suggestion for Further Reading 249
6.12.3 Open Problems 250
6.12.4 Exercises 250

7 Cryptographic Protocols 255

8 * New Frontiers 257

9 The Effect of Cryptography on Complexity Theory 259

10 * Related Topics 261

A Annotated List of References (compiled Feb. 1989) 263

A.1 General 269
A.2 Hard Computational Problems 269
A.3 Encryption 272
A.4 Pseudorandomness 273
A.5 Signatures and Commitment Schemes 275
A.6 Interactive Proofs, Zero-Knowledge and Protocols 276
A.7 Additional Topics 285
A.8 Historical Background 290