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