Contents

1 A Brief Introduction to Zero-Knowledge (by O.G.) 1
1.1 Preliminaries 3
1.1.1 Interactive Proofs and Argument Systems 4
1.1.2 Computational Difficulty and One-Way Functions 6
1.1.3 Computational Indistinguishability 7
1.2 Definitional Issues 8
1.2.1 The Simulation Paradigm 9
1.2.2 The Basic Definition 10
1.2.3 Variants 11
1.3 Zero-Knowledge Proofs for Every NP-set 15
1.3.1 Constructing Zero-Knowledge Proofs for NP-sets 15
1.3.2 Using Zero-Knowledge Proofs for NP-sets 17
1.4 Composing Zero-Knowledge Protocols 18
1.4.1 Sequential Composition 19
1.4.2 Parallel Composition 20
1.4.3 Concurrent Composition (With and Without Timing) 22

2 Introduction to Concurrent Zero-Knowledge 25
2.1 Zero-Knowledge Proof Systems 26
2.1.1 Concurrent Composition of $\mathcal{ZK}$ 26
2.1.2 On the Feasibility of $c\mathcal{ZK}$ 27
2.1.3 The Round-Complexity of $c\mathcal{ZK}$ 27
2.2 From Repetition to Composition 28
2.2.1 A “Typical” $\mathcal{ZK}$ Protocol for $\mathcal{NP}$ 29
2.2.2 Composition of $\mathcal{ZK}$ Protocols 32
2.3 A Second Look at the Feasibility of $c\mathcal{ZK}$ 33
2.3.1 A Troublesome Scheduling 33
2.3.2 The Richardson–Kilian Protocol and Its Analysis 35
2.3.3 Improving the Analysis of the RK Protocol 36
2.3.4 What About Non-Black-Box Simulation? 36
2.4 Organization and the Rest of This Book 37

3 Preliminaries 39
3.1 General 39
3.1.1 Basic Notation 39
3.1.2 Probabilistic Notation 39
3.1.3 Computational Indistinguishability 39
3.2 Interactive Proofs 40
3.3 Zero-Knowledge 41
3.4 Witness Indistinguishability 41
3.5 Concurrent Zero-Knowledge 42
3.6 Black-Box Concurrent Zero-Knowledge 43
3.7 Conventions Used in Construction of Simulators 44
3.8 Commitment Schemes 46

4 $c\mathcal{ZK}$ Proof Systems for $\mathcal{NP}$ 49
4.1 Blum's Hamiltonicity Protocol 50
4.2 The Richardson–Kilian $c\mathcal{ZK}$ Protocol 51
4.3 The Prabhakharan–Rosen–Sahai $c\mathcal{ZK}$ Protocol 53
4.4 Simulating the RK and PRS Protocols – Outline 55
4.5 Analyzing the Simulation – Outline 58
4.5.1 The Simulator Runs in Polynomial Time 59
4.5.2 The Simulator's Output is "Correctly" Distributed 59
4.5.3 The Simulator (Almost) Never Gets "Stuck" 59

5 $c\mathcal{ZK}$ in Logarithmically Many Rounds 67
5.1 Detailed Description of the Simulator 67
5.1.1 The Main Procedure and Ideas 68
5.1.2 The Actual Simulator 74
5.2 The Simulator's Running Time 75
5.3 The Simulator's Output Distribution 75
5.4 The Probability of Getting "Stuck" 77
5.4.1 Counting Bad Random Tapes 83
5.4.2 Special Intervals Are Visited Many Times 90
5.5 Extensions 95
5.5.1 Applicability to Other Protocols 95
5.5.2 $c\mathcal{ZK}$ Arguments Based on Any One-Way Function 96
5.5.3 Applicability to Resettable Zero-Knowledge 98
5.5.4 $c\mathcal{ZK}$ Arguments with Poly-Logarithmic Efficiency 99

6 A Simple Lower Bound 101
6.1 Proof of Theorem 6.1 101
6.1.1 Schedule, Adversary Verifiers and Decision Procedure .. 102
6.1.2 Proof of Lemma 6.1.5 105
6.1.3 Existence of Useful Initiation Prefixes 107
6.1.4 The Structure of Good Subtrees 109

7 Black-Box $c\mathcal{ZK}$ Requires Logarithmically Many Rounds . . . 111
7.1 Proof Outline . . . 112
7.1.1 The High-Level Framework . . . 112
7.1.2 The Schedule and Additional Ideas . . . 114
7.1.3 The Actual Analysis . . . 119
7.2 The Actual Proof . . . 119
7.2.1 The Concurrent Adversarial Verifier . . . 119
7.2.2 The Actual Verifier Strategy $V_{g,h}$ . . . 126
7.2.3 The Decision Procedure for L . . . 130
7.3 Performance on NO-instances . . . 132
7.3.1 The Cheating Prover . . . 133
7.3.2 The Success Probability of the Cheating Prover . . . 137
7.3.3 Legal Transcripts Yield Useful Block Prefixes . . . 142
7.3.4 Existence of Potentially Useful Block Prefixes . . . 144
7.3.5 Existence of Useful Block Prefixes . . . 152

8 Conclusions and Open Problems . . . 161
8.1 Avoiding the Lower Bounds of Chapter 7 . . . 161
8.2 Open Problems . . . 162

9 A Brief Account of Other Developments (by O.G.) . . . 165
9.1 Using the Adversary's Program in the Proof of Security . . . 167
9.2 Witness Indistinguishability and the FLS-Technique . . . 169
9.3 Proofs of Knowledge . . . 171
9.3.1 How to Define Proofs of Knowledge . . . 171
9.3.2 How to Construct Proofs of Knowledge . . . 172
9.4 Non-interactive Zero-Knowledge . . . 173
9.5 Statistical Zero-Knowledge . . . 174
9.5.1 Transformations . . . 175
9.5.2 Complete Problems and Structural Properties . . . 176
9.6 Resettability of a Party's Random-Tape (rZK and rsZK) . . . 176
9.7 Zero-Knowledge in Other Models . . . 177

References . . . 179