# Contents

## 1 A Brief Introduction to Zero-Knowledge (by O.G.)

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

2.1 Zero-Knowledge Proof Systems .................. 26
   2.1.1 Concurrent Composition of ZK ............... 26
   2.1.2 On the Feasibility of cZK .................... 27
   2.1.3 The Round-Complexity of cZK ................. 27

2.2 From Repetition to Composition ............... 28
   2.2.1 A “Typical” ZK Protocol for NP ............... 29
   2.2.2 Composition of ZK Protocols .................. 32

2.3 A Second Look at the Feasibility of cZK .......... 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

- **General**
  - **Basic Notation**
  - **Probabilistic Notation**
  - **Computational Indistinguishability**
- **Interactive Proofs**
- **Zero-Knowledge**
- **Witness Indistinguishability**
- **Concurrent Zero-Knowledge**
- **Black-Box Concurrent Zero-Knowledge**
- **Conventions Used in Construction of Simulators**
- **Commitment Schemes**

### 4 $cZK$ Proof Systems for $NP$

- **Blum’s Hamiltonicity Protocol**
- **The Richardson–Kilian $cZK$ Protocol**
- **The Prabhakaran–Rosen–Sahai $cZK$ Protocol**
- **Simulating the RK and PRS Protocols – Outline**
- **Analyzing the Simulation – Outline**
  - **The Simulator Runs in Polynomial Time**
  - **The Simulator’s Output is “Correctly” Distributed**
  - **The Simulator (Almost) Never Gets “Stuck”**

### 5 $cZK$ in Logarithmically Many Rounds

- **Detailed Description of the Simulator**
  - **The Main Procedure and Ideas**
  - **The Actual Simulator**
- **The Simulator’s Running Time**
- **The Simulator’s Output Distribution**
- **The Probability of Getting “Stuck”**
  - **Counting Bad Random Tapes**
  - **Special Intervals Are Visited Many Times**
- **Extensions**
  - **Applicability to Other Protocols**
  - **$cZK$ Arguments Based on Any One-Way Function**
  - **Applicability to Resettable Zero-Knowledge**
  - **$cZK$ Arguments with Poly-Logarithmic Efficiency**

### 6 A Simple Lower Bound

- **Proof of Theorem 6.1**
  - **Schedule, Adversary Verifiers and Decision Procedure**
  - **Proof of Lemma 6.1.5**
  - **Existence of Useful Initiation Prefixes**
  - **The Structure of Good Subtrees**
7  Black-Box \( cZK \) 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 \( \text{no} \)-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