

# Contents

|          |                                                                         |           |
|----------|-------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Introduction</b>                                                     | <b>1</b>  |
| 1.1      | Background and Aims . . . . .                                           | 1         |
| 1.1.1    | Introductory Comments . . . . .                                         | 1         |
| 1.1.2    | Discussion of Public-key and Private-key Cryptography                   | 2         |
| 1.1.3    | Digital Signature . . . . .                                             | 5         |
| 1.1.4    | RSA Cryptosystem and Digital Signature . . . . .                        | 9         |
| 1.1.5    | Signature-Hashing Scheme . . . . .                                      | 10        |
| 1.1.6    | Other Applications of Hash Functions . . . . .                          | 13        |
| 1.2      | Contents of the Book . . . . .                                          | 14        |
| <b>2</b> | <b>Overview of Hash Functions</b>                                       | <b>18</b> |
| 2.1      | Introduction . . . . .                                                  | 18        |
| 2.2      | Properties of Secure Hash Functions . . . . .                           | 19        |
| 2.3      | Definitions . . . . .                                                   | 20        |
| 2.3.1    | Strong and Weak Hash Functions . . . . .                                | 20        |
| 2.3.2    | Message Authentication Codes and Manipulation Detection Codes . . . . . | 22        |
| 2.3.3    | Block-cipher-based and Non-block-cipher-based Hash Functions . . . . .  | 23        |
| 2.4      | Block-cipher-based Hash Functions . . . . .                             | 24        |

|          |                                                       |           |
|----------|-------------------------------------------------------|-----------|
| 2.4.1    | Rabin's Scheme . . . . .                              | 25        |
| 2.4.2    | Cipher Block Chaining Scheme . . . . .                | 26        |
| 2.4.3    | CBC with Checksum Scheme . . . . .                    | 26        |
| 2.4.4    | Combined Plaintext-Ciphertext Chaining Scheme . . .   | 27        |
| 2.4.5    | Key Chaining Scheme . . . . .                         | 28        |
| 2.4.6    | Winternitz' Key Chaining Schemes . . . . .            | 29        |
| 2.4.7    | Quisquater and Girault's 2n-bit Hash Function . . . . | 30        |
| 2.4.8    | Merkle's Scheme . . . . .                             | 31        |
| 2.4.9    | N-hash Algorithm . . . . .                            | 32        |
| 2.4.10   | MDC2 and MDC4 . . . . .                               | 33        |
| 2.5      | Non-block-cipher-based Hash Functions . . . . .       | 34        |
| 2.5.1    | Cipher Block Chaining with RSA . . . . .              | 35        |
| 2.5.2    | Schemes Based on Squaring . . . . .                   | 36        |
| 2.5.3    | Schemes Based on Claw-Free Permutations . . . . .     | 38        |
| 2.5.4    | Schemes Based on the Knapsack Problem . . . . .       | 39        |
| 2.5.5    | Schemes Based on Cellular Automata . . . . .          | 40        |
| 2.5.6    | Software Hash Schemes . . . . .                       | 41        |
| 2.5.7    | Matrix Hashing . . . . .                              | 43        |
| 2.5.8    | Schnorr's FFT Hashing Scheme . . . . .                | 44        |
| 2.6      | Design Principles for Hash Functions . . . . .        | 45        |
| 2.6.1    | Serial Method . . . . .                               | 45        |
| 2.6.2    | Parallel Method . . . . .                             | 46        |
| 2.7      | Conclusions . . . . .                                 | 46        |
| <b>3</b> | <b>Methods of Attack on Hash Functions</b>            | <b>48</b> |
| 3.1      | Introduction . . . . .                                | 48        |

|          |                                                             |           |
|----------|-------------------------------------------------------------|-----------|
| 3.2      | General Attacks . . . . .                                   | 49        |
| 3.3      | Special Attacks . . . . .                                   | 50        |
| 3.3.1    | Meet-in-the-middle Attack . . . . .                         | 51        |
| 3.3.2    | Generalized Meet-in-the-middle Attack . . . . .             | 52        |
| 3.3.3    | Correcting Block Attack . . . . .                           | 53        |
| 3.3.4    | Attacks Depending on Algorithm Weaknesses . . . . .         | 53        |
| 3.3.5    | Differential Cryptanalysis . . . . .                        | 54        |
| 3.4      | Conclusions . . . . .                                       | 54        |
| <b>4</b> | <b>Pseudorandomness</b>                                     | <b>56</b> |
| 4.1      | Introduction . . . . .                                      | 56        |
| 4.2      | Notation . . . . .                                          | 58        |
| 4.3      | Indistinguishability . . . . .                              | 58        |
| 4.4      | Pseudorandom Bit Generators . . . . .                       | 60        |
| 4.5      | Pseudorandom Function Generators . . . . .                  | 62        |
| 4.6      | Pseudorandom Permutation Generators . . . . .               | 66        |
| 4.6.1    | Construction . . . . .                                      | 66        |
| 4.6.2    | Improvements and Implications . . . . .                     | 69        |
| 4.6.3    | Security . . . . .                                          | 72        |
| 4.7      | Conclusions . . . . .                                       | 76        |
| <b>5</b> | <b>Construction of Super-Pseudorandom Permutations</b>      | <b>77</b> |
| 5.1      | Introduction . . . . .                                      | 77        |
| 5.2      | Super-Pseudorandom Permutations . . . . .                   | 78        |
| 5.3      | Necessary and Sufficient Conditions . . . . .               | 79        |
| 5.4      | Super-Pseudorandomness in Generalized DES-like Permutations | 92        |
| 5.4.1    | Feistel-Type Transformations . . . . .                      | 93        |

|          |                                                                                  |            |
|----------|----------------------------------------------------------------------------------|------------|
| 5.4.2    | Super-Pseudorandomness of Type-1 Transformations . . . . .                       | 96         |
| 5.5      | Conclusions and Open Problems . . . . .                                          | 103        |
| <b>6</b> | <b>A Sound Structure</b>                                                         | <b>105</b> |
| 6.1      | Introduction . . . . .                                                           | 105        |
| 6.2      | Preliminaries . . . . .                                                          | 106        |
| 6.3      | Perfect Randomizers . . . . .                                                    | 112        |
| 6.4      | A Construction for Super-Pseudorandom Permutation Generators . . . . .           | 116        |
| 6.4.1    | Super-Pseudorandomness of $\psi(h, 1, f, h, 1, f)$ . . . . .                     | 117        |
| 6.4.2    | Super-Pseudorandomness of $\psi(f^2, 1, f, f^2, 1, f)$ . . . . .                 | 124        |
| 6.5      | Conclusions and Open Problems . . . . .                                          | 130        |
| <b>7</b> | <b>A Construction for One Way Hash Functions and Pseudorandom Bit Generators</b> | <b>132</b> |
| 7.1      | Introduction . . . . .                                                           | 132        |
| 7.2      | Notation . . . . .                                                               | 134        |
| 7.3      | Preliminaries . . . . .                                                          | 135        |
| 7.4      | Theoretic Constructions . . . . .                                                | 137        |
| 7.4.1    | Naor and Yung's Scheme . . . . .                                                 | 138        |
| 7.4.2    | Zheng, Matsumoto and Imai's First Scheme . . . . .                               | 138        |
| 7.4.3    | De Santis and Yung's Schemes . . . . .                                           | 139        |
| 7.4.4    | Rompel's Scheme . . . . .                                                        | 140        |
| 7.5      | Hard Bits and Pseudorandom Bit Generation . . . . .                              | 140        |
| 7.6      | A Strong One-Way Permutation . . . . .                                           | 146        |
| 7.7      | UOWHF Construction and PBG . . . . .                                             | 151        |
| 7.7.1    | UOWHF Based on the Strong One-way Permutation . . . . .                          | 152        |

|          |                                                                 |            |
|----------|-----------------------------------------------------------------|------------|
| 7.7.2    | Parameterization . . . . .                                      | 153        |
| 7.7.3    | Compressing Arbitrary Length Messages . . . . .                 | 154        |
| 7.8      | A Single construction for UOWHF and PBG . . . . .               | 155        |
| 7.9      | Conclusions and Extensions . . . . .                            | 156        |
| <b>8</b> | <b>How to Construct a Family of Strong One Way Permutations</b> | <b>157</b> |
| 8.1      | Introduction . . . . .                                          | 157        |
| 8.2      | Preliminary Comments . . . . .                                  | 159        |
| 8.3      | Strong One Way Permutations . . . . .                           | 162        |
| 8.3.1    | A Scheme for the Construction of Strong Permutations            | 164        |
| 8.3.2    | A Three-layer Construction for Strong Permutations .            | 166        |
| 8.4      | Conclusions . . . . .                                           | 168        |
| <b>9</b> | <b>Conclusions</b>                                              | <b>170</b> |
| 9.1      | Summary . . . . .                                               | 170        |
| 9.2      | Limitations and Assumptions of the Results . . . . .            | 174        |
| 9.3      | Prospects for Further Research . . . . .                        | 177        |
|          | <b>Bibliography</b>                                             | <b>179</b> |
|          | <b>Index</b>                                                    | <b>191</b> |