

# Contents

|          |                                                                       |           |
|----------|-----------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Requirements on Digital Signature Schemes.....</b>                 | <b>1</b>  |
| 1.1      | Brief Survey of Applications.....                                     | 1         |
| 1.2      | Legal Significance of Signatures .....                                | 2         |
| 1.3      | Consequences of the Legal Significance.....                           | 4         |
| 1.4      | Secure Hardware Support.....                                          | 6         |
| 1.5      | Relation to Other Types of Schemes .....                              | 8         |
| 1.6      | A Variant: Invisible Signatures .....                                 | 10        |
| <br>     |                                                                       |           |
| <b>2</b> | <b>History of Digital Signature Schemes .....</b>                     | <b>11</b> |
| 2.1      | Classical Cryptography .....                                          | 11        |
| 2.2      | Information-Theoretically Secure Symmetric Schemes .....              | 12        |
| 2.3      | Invention of Digital Signature Schemes .....                          | 13        |
| 2.4      | Intuitively Constructed Digital Signature Schemes .....               | 18        |
| 2.5      | Problems, Countermeasures, and Emerging Security Notions .....        | 22        |
| 2.6      | “Provably Secure” Digital Signature Schemes .....                     | 25        |
| 2.7      | Special Variants.....                                                 | 28        |
| 2.7.1    | Special Signature Schemes .....                                       | 28        |
| 2.7.2    | Signature-Related Schemes.....                                        | 29        |
| <br>     |                                                                       |           |
| <b>3</b> | <b>Information-Theoretic Security for Signers: Introduction .....</b> | <b>33</b> |
| 3.1      | Problems with Ordinary Digital Signature Schemes .....                | 33        |
| 3.2      | One New Type: Fail-Stop Signature Schemes .....                       | 35        |
| <br>     |                                                                       |           |
| <b>4</b> | <b>Terminology .....</b>                                              | <b>37</b> |
| 4.1      | General Notation .....                                                | 37        |
| 4.2      | Probabilities and Probabilistic Functions .....                       | 37        |
| 4.3      | Complexity .....                                                      | 38        |
| 4.4      | Interaction .....                                                     | 40        |
| 4.4.1    | Overview and Meta-Terminology.....                                    | 40        |
| 4.4.2    | Some Terminology about Specifications.....                            | 41        |
| 4.4.3    | Interactive Functions and Algorithms .....                            | 42        |
| 4.4.4    | System Structure.....                                                 | 44        |
| 4.4.5    | Attackers .....                                                       | 45        |
| 4.4.6    | System Behaviour .....                                                | 45        |
| 4.4.7    | Degrees of Fulfilling .....                                           | 46        |
| <br>     |                                                                       |           |
| <b>5</b> | <b>Properties of Digital Signature Schemes .....</b>                  | <b>47</b> |
| 5.1      | The Main Ideas .....                                                  | 48        |
| 5.1.1    | The Ideas and their Background .....                                  | 48        |

|        |                                                                      |     |
|--------|----------------------------------------------------------------------|-----|
| 5.1.2  | Problems, Alternatives, and Simplification .....                     | 51  |
| 5.2    | Service .....                                                        | 55  |
| 5.2.1  | What Kind of Specification? .....                                    | 56  |
| 5.2.2  | Overview of the Services of Signature Schemes .....                  | 58  |
| 5.2.3  | Remarks on the Generality of the Definition .....                    | 62  |
| 5.2.4  | Interface Events in Detail .....                                     | 64  |
| 5.2.5  | Specification and System Parameters .....                            | 72  |
| 5.2.6  | Towards Formalizations of Requirements .....                         | 75  |
| 5.2.7  | Minimal Requirements .....                                           | 81  |
| 5.2.8  | Stronger Requirements .....                                          | 88  |
| 5.2.9  | Multiple Specifications for Different Degrees of Security .....      | 91  |
| 5.2.10 | Special Specification Parameters .....                               | 96  |
| 5.2.11 | Additional Transactions .....                                        | 97  |
| 5.2.12 | Privacy Requirements .....                                           | 102 |
| 5.3    | Structure .....                                                      | 103 |
| 5.3.1  | Minimal Structural Requirements .....                                | 104 |
| 5.3.2  | Additional Structural Properties .....                               | 105 |
| 5.4    | Security .....                                                       | 109 |
| 5.4.1  | Access of Attackers to System Parts .....                            | 110 |
| 5.4.2  | Influence of Attackers on Honest Users .....                         | 112 |
| 5.4.3  | Computational Assumptions and Notions of Fulfilling .....            | 116 |
| 5.4.4  | Sketches of Expected Theorems and Proofs .....                       | 121 |
| 6      | Overview of Existing Schemes with Other than Ordinary Security ..... | 125 |
| 6.1    | Properties .....                                                     | 125 |
| 6.1.1  | Top-Level Classification .....                                       | 125 |
| 6.1.2  | Fail-Stop Signature Schemes .....                                    | 126 |
| 6.1.3  | Invisible Signature Schemes with Dual Security .....                 | 131 |
| 6.1.4  | “Normal” Signature Schemes with Dual Security .....                  | 132 |
| 6.1.5  | Schemes with Information-Theoretic Security .....                    | 133 |
| 6.2    | Possible Applications and Legal Significance .....                   | 134 |
| 6.2.1  | Possible Benefits of Dual Security .....                             | 135 |
| 6.2.2  | Possible Benefits of Fail-Stop Security .....                        | 138 |
| 6.3    | Important Construction Ideas .....                                   | 139 |
| 6.3.1  | Construction of Fail-Stop Signature Schemes .....                    | 140 |
| 6.3.2  | Construction of Invisible Signature Schemes with Dual Security ..... | 145 |
| 6.3.3  | Construction of “Normal” Signature Schemes with Dual Security .....  | 146 |
| 6.3.4  | Construction of Schemes with Information-Theoretic Security .....    | 147 |

|          |                                                                                                      |            |
|----------|------------------------------------------------------------------------------------------------------|------------|
| <b>7</b> | <b>Conventional Definitions of Fail-Stop Signature Schemes and General Reductions .....</b>          | <b>149</b> |
| 7.1      | Definition .....                                                                                     | 149        |
| 7.1.1    | Concentrating on Schemes with Special Risk Bearers .....                                             | 150        |
| 7.1.2    | Top-Down Derivation of the Components .....                                                          | 150        |
| 7.1.3    | Breaking Down the Minimal Requirements .....                                                         | 161        |
| 7.1.4    | Breaking Down Additional Service Properties .....                                                    | 166        |
| 7.1.5    | Formal Security Definitions .....                                                                    | 168        |
| 7.2      | Relations Between Security Properties .....                                                          | 175        |
| 7.2.1    | Security for the Signer “Backwards” .....                                                            | 175        |
| 7.2.2    | Unforgeability .....                                                                                 | 180        |
| 7.3      | Fail-Stop Signature Schemes with Prekey .....                                                        | 184        |
| 7.3.1    | Appropriate Zero-Knowledge Proof Schemes .....                                                       | 185        |
| 7.3.2    | Definition of Schemes with Prekey .....                                                              | 192        |
| 7.3.3    | Security of Schemes with Prekey .....                                                                | 196        |
| 7.4      | Relation to Ordinary Digital Signature Schemes .....                                                 | 201        |
| 7.5      | Constructions with Many Risk Bearers .....                                                           | 203        |
| 7.5.1    | Replication of Initialization .....                                                                  | 203        |
| 7.5.2    | Multi-Party Function Evaluation in Initialization .....                                              | 207        |
| <b>8</b> | <b>Building Blocks .....</b>                                                                         | <b>213</b> |
| 8.1      | Some Group and Number Theory .....                                                                   | 213        |
| 8.1.1    | Basic Facts from Group Theory .....                                                                  | 213        |
| 8.1.2    | Basic Facts about Rings of Integers Modulo $n$ .....                                                 | 214        |
| 8.1.3    | Generalized Blum Integers .....                                                                      | 216        |
| 8.1.4    | Williams Integers .....                                                                              | 217        |
| 8.1.5    | The Density of Primes .....                                                                          | 217        |
| 8.2      | Functions with Large Preimage Sets .....                                                             | 218        |
| 8.2.1    | Discrete-Logarithm Case: Tuple Exponentiation .....                                                  | 219        |
| 8.2.2    | A Construction from Pairs of Permutations .....                                                      | 221        |
| 8.2.3    | Factoring Case: Iterated Squaring and Doubling<br>(Or: A Useful Homomorphism on an Ugly Group) ..... | 223        |
| 8.3      | Some Efficient Algorithms .....                                                                      | 228        |
| 8.4      | Concrete Cryptologic Assumptions .....                                                               | 230        |
| 8.4.1    | Integer Factoring .....                                                                              | 230        |
| 8.4.2    | Discrete Logarithm .....                                                                             | 233        |
| 8.5      | Collision-Intractable Function Families .....                                                        | 240        |
| 8.5.1    | Overview .....                                                                                       | 240        |
| 8.5.2    | Definitions .....                                                                                    | 244        |
| 8.5.3    | Constructions in the Discrete-Logarithm Case .....                                                   | 253        |
| 8.5.4    | Constructions from Claw-Intractable Pairs of<br>Permutations .....                                   | 273        |
| 8.5.5    | Constructions in the Factoring Case .....                                                            | 282        |

|           |                                                                             |            |
|-----------|-----------------------------------------------------------------------------|------------|
| <b>9</b>  | <b>Constructions for One Message Block.....</b>                             | <b>289</b> |
| 9.1       | Definition of Schemes for Signing Message Blocks .....                      | 289        |
| 9.2       | General Construction Framework .....                                        | 290        |
| 9.3       | Implementation Based on the Discrete-Logarithm Assumption .....             | 299        |
| 9.4       | Implementations Based on the Factoring Assumption .....                     | 304        |
| 9.5       | Complexity Overview .....                                                   | 311        |
| <b>10</b> | <b>Signing Many Long Messages .....</b>                                     | <b>313</b> |
| 10.1      | Message Hashing .....                                                       | 313        |
| 10.2      | Bottom-up Tree Authentication .....                                         | 322        |
| 10.3      | Top-Down Tree Authentication .....                                          | 325        |
| 10.4      | Top-Down Tree Authentication with Small Amount of Private<br>Storage .....  | 332        |
| 10.5      | Discrete-Logarithm Scheme with Shorter Secret Key .....                     | 339        |
| 10.6      | The Case of a Fixed Recipient .....                                         | 343        |
| <b>11</b> | <b>Lower Bounds .....</b>                                                   | <b>345</b> |
| 11.1      | Information-Theoretic Background.....                                       | 346        |
| 11.2      | Random Variables in Fail-Stop Signature Schemes .....                       | 348        |
| 11.3      | Lower Bound on the Secret Random Bits Needed .....                          | 349        |
| 11.4      | Length of Signatures and Public Keys .....                                  | 356        |
| 11.5      | Lower Bounds on Information-Theoretically Secure Signature<br>Schemes ..... | 360        |
| 11.6      | Comparison .....                                                            | 366        |
|           | <b>References .....</b>                                                     | <b>371</b> |
|           | <b>Symbols.....</b>                                                         | <b>387</b> |
|           | <b>Index .....</b>                                                          | <b>391</b> |