Contents

Foreword xi
David POINTCHEVAL

Chapter 1. Public-Key Encryption and Security Notions 1
Nuttapong ATTRAPADUNG and Takahiro MATSUDA

1.1. Basic definitions for PKE 2
1.1.1. Basic notation 2
1.1.2. Public-key encryption 2
1.1.3. IND-CPA and IND-CCA security 2
1.1.4. Other basic security notions and relations 4
1.2. Basic PKE schemes 5
1.2.1. Game-based proofs 5
1.2.2. ElGamal encryption 6
1.2.3. Simplified CS encryption 8
1.2.4. Cramer–Shoup encryption 11
1.2.5. Other specific PKE schemes 14
1.3. Generic constructions for IND-CCA secure PKE 16
1.3.1. Hybrid encryption 17
1.3.2. Naor–Yung construction and extensions 19
1.3.3. Fujisaki–Okamoto and other transforms in the RO model 21
1.3.4. Other generic constructions for IND-CCA secure PKE 23
1.4. Advanced topics 25
1.4.1. Intermediate notions related to CCA 25
1.4.2. IND-CCA security in multi-user setting and tight security 26
1.4.3. Key-dependent message security 28
1.4.4. More topics on PKE 30
1.5. References 31

Chapter 2. Signatures and Security Notions 47
Marc FISCHLIN

2.1. Signature schemes 47
2.1.1. Definition 47
2.1.2. Examples of practical schemes 49
2.2. Unforgeability 51
2.2.1. Discussion 51
2.2.2. Existential unforgeability under chosen-message attacks 53
2.2.3. Unforgeability of practical schemes 54
2.3. Strong unforgeability 56
2.3.1. Discussion 56
2.3.2. Strong existential unforgeability under chosen-message attacks . . 57
2.3.3. Strong unforgeability of practical schemes 58
2.3.4. Building strongly unforgeable schemes 59
2.4. Summary 60
2.5. References 60

Chapter 3. Zero-Knowledge Proofs 63
Ivan VISCONTI

3.1. Introduction 63
3.2. Notation 64
3.3. Classical zero-knowledge proofs 64
3.3.1. Zero knowledge 65
3.4. How to build a zero-knowledge proof system 68
3.4.1. ZK proofs for all $\mathcal{NP}$ 70
3.4.2. Round complexity 71
3.5. Relaxed security in proof systems 72
3.5.1. Honest-verifier ZK 72
3.5.2. Witness hiding/indistinguishability 73
3.5.3. Σ-Protocols 74
3.6. Non-black-box zero knowledge 75
3.7. Advanced notions 75
3.7.1. Publicly verifiable zero knowledge 76
3.7.2. Concurrent ZK and more 77
3.7.3. ZK with stateless players 78
3.7.4. Delayed-input proof systems 79
3.8. Conclusion 80
3.9. References 80

Chapter 4. Secure Multiparty Computation 85
Yehuda LINDELL

4.1. Introduction 85
4.1.1. A note on terminology 87
4.2. Security of MPC 87
4.2.1. The definitional paradigm 87
4.2.2. Additional definitional parameters 89
4.2.3. Adversarial power 89
4.2.4. Modular sequential and concurrent composition 91
4.2.5. Important definitional implications 92
4.2.6. The ideal model and using MPC in practice 92
4.2.7. Any inputs are allowed 92
4.2.8. MPC secures the process, but not the output 92
4.3. Feasibility of MPC 93
4.4. Techniques 94
4.4.1. Shamir secret sharing 94
4.4.2. Honest-majority MPC with secret sharing 95
4.4.3. Private set intersection 97
4.4.4. Threshold cryptography 99
4.4.5. Dishonest-majority MPC 100
4.4.6. Efficient and practical MPC 100
4.5. MPC use cases 101
4.5.1. Boston wage gap (Lapets et al. 2018) 101
4.5.2. Advertising conversion (Ion et al. 2017) 101
4.5.3. MPC for cryptographic key protection (Unbound Security; Sepior; Curv) 101
4.5.4. Government collaboration (Sharemind) 102
4.5.5. Privacy-preserving analytics (Duality) 102
4.6. Discussion 102
4.7. References 103

Chapter 5. Pairing-Based Cryptography 107
Olivier BLAZY

5.1. Introduction 108
5.1.1. Notations 108
5.1.2. Generalities 108
5.2. One small step for man, one giant leap for cryptography 109
5.2.1. Opening Pandora's box, demystifying the magic 110
5.2.2. A new world of assumptions 112
5.3. A new world of cryptographic protocols at your fingertips 116
5.3.1. Identity-based encryption made easy 117

5.3.2. Efficient deterministic compact signature 118
5.4. References 119

Chapter 6. Broadcast Encryption and Traitor Tracing 121
Duong HIEU PHAN

6.1. Introduction 121
6.2. Security notions for broadcast encryption and TT 123
6.3. Overview of broadcast encryption and TT 125
6.4. Tree-based methods 129
6.5. Code-based TT 132
6.6. Algebraic schemes 135
6.7. Lattice-based approach with post-quantum security 142
6.8. References 143

Chapter 7. Attribute-Based Encryption 151
Romain GAY

7.1. Introduction 151
7.2. Pairing groups 152
7.2.1. Cyclic groups 152
7.2.2. Pairing groups 152
7.3. Predicate encodings 153
7.3.1. Definition 153
7.3.2. Constructions 154
7.4. Attribute-based encryption 156
7.4.1. Definition 156
7.4.2. A modular construction 158
7.5. References 165

Chapter 8. Advanced Signatures 167
Olivier SANDERS

8.1. Introduction 167
8.2. Some constructions 169
8.2.1. The case of scalar messages 169
8.2.2. The case of non-scalar messages 171
8.3. Applications 173
8.3.1. Anonymous credentials 173
8.3.2. Group signatures 176
8.3.3. Direct anonymous attestations 180
8.4. References 184

Chapter 9. Key Exchange 187
Colin BOYD

9.1. Key exchange fundamentals 187
9.1.1. Key exchange parties 188
9.1.2. Key exchange messages 189
9.1.3. Key derivation functions 189
9.2. Unauthenticated key exchange 191
9.2.1. Formal definitions and security models 191
9.2.2. Constructions and examples 192
9.3. Authenticated key exchange 194
9.3.1. Non-interactive key exchange 195
9.3.2. AKE security models 196
9.3.3. Constructions and examples 200
9.4. Conclusion 206
9.5. References 207

Chapter 10. Password Authenticated Key Exchange: Protocols and Security Models 213
Stanislaw JARECKI

10.1. Introduction 213
10.2. First PAKE: EKE 215
10.3. Game-based model of PAKE security 218
10.3.1. The BPR security model 218
10.3.2. Implicit versus explicit authentication 221
10.3.3. Limitations of the BPR model 221
10.3.4. EKE instantiated with Diffie–Hellman KE 223
10.3.5. Implementing ideal cipher on arbitrary groups 224
10.4. Simulation-based model of PAKE security 225
10.4.1. The BMP security model 225
10.4.2. Advantages of BMP definition: arbitrary passwords, tight security 229
10.4.3. EKE using RO-derived one-time pad encryption 230
10.4.4. BMP model for PAKE with explicit authentication (PAKE-EA) 231
10.5. Universally composable model of PAKE security 232
10.6. PAKE protocols in the standard model 236
10.7. PAKE efficiency optimizations 239
10.8. Asymmetric PAKE: PAKE for the client-server setting 242
10.9. Threshold PAKE 244
10.10. References 246

Chapter 11. Verifiable Computation and Succinct Arguments for NP 257
Dario FIORE

11.1. Introduction 257
11.1.1. Background 258
11.2. Preliminaries 259
11.3. Verifiable computation 260
11.4. Constructing VC 261
11.4.1. VC for circuits in three steps 261
11.4.2. Succinct non-interactive arguments for non-deterministic computation 263
11.4.3. Verifiable computation from SNARG 264
11.5. A modular construction of SNARGs 264
11.5.1. Algebraic non-interactive linear proofs 265
11.5.2. Bilinear groups 267
11.5.3. SNARGs from algebraic NILPs with degree-2 verifiers using bilinear groups 269
11.6. Constructing algebraic NILPs for arithmetic circuits 271
11.6.1. Arithmetic circuits 271
11.6.2. Quadratic arithmetic programs 271
11.6.3. Algebraic NILP for QAPs 274
11.7. Conclusion 279
11.8. References 279

List of Authors 283

Index 285