Contents

Preface xiii
Emmanuel PROUFF, Guénaël RENAULT, Matthieu RIVAIN
and Colin O'FLYNN

Part 1. White-Box Cryptography 1

Chapter 1. Introduction to White-Box Cryptography 3
Pierre GALISSANT and Louis GOUBIN

1.1. Introductory remarks 3
1.2. Basic notions for white-box cryptography 6
1.2.1. Unbreakability 6
1.2.2. Incompressibility 7
1.2.3. One-wayness 8
1.3. Proposed (and broken) solutions 9
1.3.1. Block ciphers 9
1.3.2. Asymmetric algorithms 10
1.4. Generic strategies to build white-box implementations 12
1.4.1. DCA and countermeasures 12
1.4.2. Using fully homomorphic encryption (FHE) 13
1.4.3. White-box solutions with the help of a (small) tamper-resistant hardware 14
1.5. Applications of white-box cryptography 15
1.5.1. EMV payments on NFC-enabled smartphones without secure element 15
1.5.2. Software DRM mechanisms for digital contents 16
1.5.3. Mobile contract signing 16
1.5.4. Cryptocurrencies and blockchain technologies 16
1.6. Notes and further references 17
1.7. References 19

Chapter 2. Gray-Box Attacks against White-Box Implementations 23
Aleksei UDOVENKO

2.1. Introduction 23
2.2. Specifics of white-box side-channels 24
2.2.1. Determinism 25
2.2.2. Precise measurements 25
2.2.3. Data-dependency graph and attack windows 25
2.2.4. Computational model 26
2.2.5. Computational traces 28
2.2.6. Sensitive/predictable functions 28
2.3. Fault injections 30
2.3.1. Locating and removing pseudorandomness and dummy values 31
2.3.2. Detecting linear shares from output collisions 33
2.4. Exact matching attack 35
2.4.1. First-order exact matching attack 35
2.4.2. Higher order exact matching attack 37
2.5. Linear decoding analysis/algebraic attacks 39
2.5.1. Basic algebraic attack 39
2.5.2. Differential algebraic attack against shuffling 40
2.6. Countermeasures against the algebraic attack 43
2.6.1. Security model sketch 43
2.6.2. Nonlinear masking 45
2.6.3. Dummy shuffling 47
2.7. Conclusions 49
2.8. Notes and further references 50
2.9. References 50

Chapter 3. Tools for White-Box Cryptanalysis 53
Philippe TEUWEN

3.1. Introduction 53
3.2. Tracing programs 55
3.3. Target recognition 57
3.4. Acquiring traces for side-channel analysis 59
3.5. Preprocessing traces 61
3.6. Differential computation analysis 62
3.7. Linear decoding analysis also known as algebraic attack 64
3.8. Injecting faults 65
3.9. Differential fault analysis 67
3.10. Coping with external encodings 69
3.11. Conclusion 70

3.12. Notes and further references 70
3.13. References 72

Chapter 4. Code Obfuscation 73
Sebastian SCHRITTWIESER and Stefan KATZENBEISSER

4.1. Introduction 73
4.1.1. Definition of obfuscation 73
4.1.2. Goals of obfuscation 74
4.1.3. Protecting against locating data 74
4.1.4. Protecting against locating code 74
4.1.5. Protecting against extraction of code 74
4.1.6. Protecting against understanding of code 75
4.1.7. Attacker models 75
4.1.8. Pattern matching 75
4.1.9. Automated static analysis 75
4.1.10. Automated dynamic analysis 76
4.1.11. Human-assisted analysis 76
4.2. Obfuscation methods 76
4.2.1. Data obfuscation 77
4.2.2. Static obfuscation 78
4.2.3. Dynamic obfuscation 84
4.3. Attacks against obfuscation 85
4.3.1. Principles of program analysis 85
4.3.2. Measuring the strength of obfuscations 86
4.4. Application of code obfuscation 87
4.4.1. Digital rights management 87
4.4.2. Intellectual property protection 88
4.4.3. Malware obfuscation 88
4.4.4. Hardware-software binding 88
4.4.5. Software diversity 89
4.5. Conclusions 89
4.6. Notes and further references 89
4.7. References 90

Part 2. Randomness and Key Generation 93

Chapter 5. True Random Number Generation 95
Viktor FISCHER, Florent BERNARD and Patrick HADDAD

5.1. Introduction 95
5.2. TRNG design 96
5.3. Randomness and sources of randomness 97
5.3.1. Example: jitter of a clock signal as a source of randomness 99
5.3.2. Stochastic model of the phase of the jittered clock signal 99

5.4. Randomness extraction and digitization 100
5.4.1. Example: oscillator-based TRNGs 102
5.5. Post-processing of the raw binary signal 104
5.5.1. Algorithmic post-processing 104
5.6. Stochastic modeling and entropy rate management of the TRNG . . . 105
5.6.1. Example: a comprehensive stochastic model of the EO-TRNG . . 107
5.6.2. Example: stochastic model of the MO-TRNG 108
5.7. TRNG testing and testing strategies 109
5.7.1. Generic (black-box) statistical tests used in cryptography 110
5.7.2. Online statistical tests 112
5.7.3. Example: dedicated online tests for the MO-TRNG 112
5.8. Conclusion 113
5.9. Notes and further references 113
5.10. References 114

Chapter 6. Pseudorandom Number Generation 115
Jean-René REINHARD and Sylvain RUHAULT

6.1. Introduction 115
6.2. PRNG with ideal noise source 116
6.2.1. Standard PRNG 117
6.2.2. Stateful PRNG 118
6.2.3. Stateful pseudorandom generator with inputs 120
6.3. PRNG with imperfect noise sources 121
6.3.1. Extractors 122
6.3.2. Robustness model of Coretti et al. (2019) 124
6.4. Standard PRNG with inputs 125
6.4.1. General architecture of NIST PRNG with inputs 125
6.4.2. Security analysis and good practices 126
6.5. Notes and further references 128
6.6. References 129

Chapter 7. Prime Number Generation and RSA Keys 131
Marc JOYE and Pascal PAILLIER

7.1. Introduction 131
7.2. Primality testing methods 133
7.3. Generation of random units 133
7.4. Generation of random primes 136
7.4.1. Probable primes 138
7.4.2. Provable primes 138
7.5. RSA key generation 140
7.6. Exercises 143

7.7. Notes and further references 144
7.8. References 146

Chapter 8. Nonce Generation for Discrete Logarithm-Based Signatures 151
Akira TAKAHASHI and Mehdi TIBOUCHI

8.1. Introduction 151
8.2. The hidden number problem and randomness failures 153
8.2.1. From Schnorr to HNP 153
8.2.2. From ECDSA to HNP 154
8.3. Lattice attacks 154
8.3.1. Lattice basics 155
8.3.2. Expressing the HNP as a lattice problem 156
8.3.3. Some recent developments 158
8.4. Fourier transform attack 160
8.4.1. Quantifying bias using discrete Fourier transform 160
8.4.2. Stretching the peak width 162
8.4.3. Range reduction algorithms 165
8.5. Preventing randomness failures 166
8.6. Notes and further references 167
8.7. Acknowledgment 169
8.8. References 169

Chapter 9. Random Error Distributions in Post-Quantum Schemes 173
Thomas PREST

9.1. Introduction 173
9.2. Why post-quantum schemes need random errors 174
9.2.1. Example 1: noisy ElGamal 175
9.2.2. Example 2: hash-then-sign 176
9.2.3. Example 3: Fiat–Shamir with aborts 177
9.3. Distributions for random errors 178
9.3.1. Uniform distributions 179
9.3.2. Fixed weight distributions 179
9.3.3. Variants of the binomial distribution 180
9.3.4. Discrete and rounded Gaussians 181
9.3.5. Randomized rejection sampling 182
9.4. Sampling algorithms 184
9.4.1. Table-based algorithms 184
9.4.2. Random permutations 186
9.4.3. Convolution-based algorithms 189
9.4.4. Polynomial approximation 190
9.4.5. Rejection methods 191

9.4.6. Masking the various algorithmic approaches 192
9.5. Notes and further references 193
9.6. References 197

Part 3. Real-World Applications 203

Chapter 10. ROCA and Minerva Vulnerabilities 205
Jan JANCAR, Petr SVENDA and Marek SYS

10.1. The Return of Coppersmith's Attack 206
10.1.1. Fingerprinting 207
10.1.2. Factorization attack 208
10.1.3. Practical impact and disclosure 210
10.1.4. Notes and further references 215
10.2. Minerva 216
10.2.1. Discovery and leakage 216
10.2.2. Cause 217
10.2.3. Attack 218
10.2.4. Impacted domains and disclosure 220
10.2.5. Notes and further references 222
10.3. References 222

Chapter 11. Security of Automotive Systems 225
Lennert WOUTERS, Benedikt GIERLICHS and Bart PRENEEL

11.1. Introduction 225
11.2. The embedded automotive attacker 226
11.3. An overview of automotive attacks 227
11.3.1. Proximity vehicle attacks 227
11.3.2. Remote vehicle attacks 229
11.3.3. Infrastructure attacks 230
11.4. Application of physical attacks in automotive security 231
11.4.1. Side-channel analysis 231
11.4.2. Fault injection 232
11.5. Case study: Tesla Model X keyless entry system 233
11.5.1. The key fob 234
11.5.2. The body control module 235
11.5.3. Putting it all together 235
11.6. Conclusion 237
11.7. References 237

Chapter 12. Practical Full Key Recovery on a Google Titan Security Key 245
Laurent IMBERT, Victor LOMNE, Camille MUTCHLER and Thomas ROCHE

12.1. Introduction 245
12.2. Preliminaries 246
12.2.1. Product description 246
12.2.2. *Google Titan Security Key* Teardown 247
12.2.3. Matching the *Google Titan Security Key* with other NXP products 247
12.2.4. Side-channel observations 248
12.3. Reverse-engineering and vulnerability of the ECDSA algorithm . . . 249
12.3.1. Reverse engineering the ECDSA signature algorithm 249
12.3.2. A sensitive leakage 251
12.4. A key-recovery attack 252
12.4.1. Recovering scalar bits from the observed leakage 253
12.4.2. Lattice-based attack with partial knowledge of the nonces 253
12.5. Take-home message 255
12.6. References 255

Chapter 13. An Introduction to Intentional Electromagnetic Interference Exploitation 257
José LOPES ESTEVES

13.1. IEMI: history and definition 257
13.2. Information security threats related to electromagnetic susceptibility 259
13.3. Electromagnetic fault injection 260
13.4. Destruction, denial of service 261
13.5. Denial of service on radio front-ends 261
13.6. Signal injection in communication interfaces 262
13.7. Signal injection attacks on sensors and actuators 262
13.8. IEMI-covert channel 263
13.8.1. The air gap 264
13.8.2. Bridging air gaps 264
13.8.3. Threat model 266
13.8.4. Practical IEMI-covert channel on a PC 266
13.9. Electromagnetic watermarking 269
13.9.1. Threat model 269
13.9.2. EMW for forensic tracking 269
13.9.3. Practical EMW on a UAV 271
13.10. Conclusion 273
13.11. References 274

Chapter 14. Attacking IoT Light Bulbs 279
Colin O'FLYNN and Eyal RONEN

14.1. Introduction 279
14.2. Preliminaries 280
14.2.1. ZLL (ZigBee Light Link) and smart light systems 280
14.2.2. Lamp hardware 281
14.2.3. Firmware updates 281
14.2.4. Hue Bridge hardware 282
14.3. Hardware AES and AES-CTR attacks 282
14.3.1. Application to ATMega128RFA1 283
14.3.2. Later-round attacks 285
14.4. AES-CCM bootloader attack 286
14.4.1. Understanding Philips OTA image cryptographic primitives . . . 286
14.4.2. CPA attack against the CCM CBC MAC verification 289
14.5. Application of attack 293
14.6. Notes and further references 294
14.7. References 295

List of Authors 297

Index 301

Summary of Volume 1 305

Summary of Volume 2 313