# Contents

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

**Part 1. Masking** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1

**Chapter 1. Introduction to Masking** . . . . . . . . . . . . . . . . . . . . . 3
Ange MARTINELLI and Mélissa ROSSI

1.1. An overview of masking . . . . . . . . . . . . . . . . . . . . . . . . . 3
1.2. The effect of masking on side-channel leakage . . . . . . . . . . . . . 4
1.3. Different types of masking . . . . . . . . . . . . . . . . . . . . . . . 5
1.4. Code-based masking: toward a generic framework . . . . . . . . . . . 8
1.5. Hybrid masking . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10
1.6. Examples of specific maskings . . . . . . . . . . . . . . . . . . . . . 11
1.7. Outline of the part . . . . . . . . . . . . . . . . . . . . . . . . . . . 12
1.8. Notes and further references . . . . . . . . . . . . . . . . . . . . . . 13
1.9. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 13

**Chapter 2. Masking Schemes** . . . . . . . . . . . . . . . . . . . . . . . . 15
Jean-Sébastien CORON and Rina ZEITOUN

2.1. Introduction to masking operations . . . . . . . . . . . . . . . . . . 15
2.2. Classical linear operations . . . . . . . . . . . . . . . . . . . . . . . 15
2.3. Classical nonlinear operations . . . . . . . . . . . . . . . . . . . . . 16
2.3.1. Application of ISW algorithm for $n = 2$ and $n = 3$ . . . . . . . . . 17
2.4. Mask refreshing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18
2.4.1. Refresh masks with complexity $\mathcal{O}(n)$ . . . . . . . . . . . . . . . 18
2.4.2. Refresh masks with complexity $\mathcal{O}(n^2)$ . . . . . . . . . . . . . . . 18
2.4.3. Refresh masks with complexity $\mathcal{O}(n \cdot \log n)$ . . . . . . . . . . . . 19

2.5. Masking S-boxes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 21
2.5.1. The Rivain–Prouff countermeasure for AES . . . . . . . . . . . . 21
2.5.2. Extension to any S-box . . . . . . . . . . . . . . . . . . . . . . . . . 22
2.5.3. The randomized table countermeasure . . . . . . . . . . . . . . . 23
2.5.4. Attacks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
2.6. Masks conversions . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27
2.6.1. First-order Boolean to arithmetic masking . . . . . . . . . . . . . 27
2.6.2. Generalization to high order for Boolean to arithmetic masking . . . . . . . . . . . . . . . . . . . . . . . . . . 28
2.6.3. High order Boolean to arithmetic and arithmetic to Boolean masking . . . . . . . . . . . . . . . . . . . . . . . . . . 30
2.7. Notes and further references . . . . . . . . . . . . . . . . . . . . . . 35
2.8. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 37

**Chapter 3. Hardware Masking** . . . . . . . . . . . . . . . . . . . . . . . 39
Begül BILGIN and Lauren DE MEYER

3.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 39
3.1.1. Glitches . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 40
3.1.2. Glitch-extended probes . . . . . . . . . . . . . . . . . . . . . . . . 41
3.1.3. Non-completeness . . . . . . . . . . . . . . . . . . . . . . . . . . . 41
3.2. Category I: $td + 1$ masking . . . . . . . . . . . . . . . . . . . . . . . 42
3.2.1. First-order security . . . . . . . . . . . . . . . . . . . . . . . . . . 43
3.2.2. Higher-order security . . . . . . . . . . . . . . . . . . . . . . . . . 46
3.3. Category II: $d + 1$ masking . . . . . . . . . . . . . . . . . . . . . . . 46
3.3.1. General construction . . . . . . . . . . . . . . . . . . . . . . . . . 47
3.3.2. Security argument . . . . . . . . . . . . . . . . . . . . . . . . . . . 48
3.3.3. Comparing to $td + 1$ masking . . . . . . . . . . . . . . . . . . . . 49
3.3.4. Higher-degree functions . . . . . . . . . . . . . . . . . . . . . . . . 50
3.4. Trade-offs . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 51
3.4.1. Minimizing area . . . . . . . . . . . . . . . . . . . . . . . . . . . . 52
3.4.2. Minimizing latency . . . . . . . . . . . . . . . . . . . . . . . . . . 52
3.4.3. Minimizing randomness . . . . . . . . . . . . . . . . . . . . . . . . 53
3.5. Notes and further references . . . . . . . . . . . . . . . . . . . . . . 53
3.6. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55

**Chapter 4. Masking Security Proofs** . . . . . . . . . . . . . . . . . . . . 59
Sonia BELAÏD

4.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 59
4.2. Preliminaries . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 60
4.2.1. Circuits . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 60
4.2.2. Additive sharings and gadgets . . . . . . . . . . . . . . . . . . . . 61
4.2.3. Compilers . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 61
4.3. Probing model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 62

4.3.1. Formal definition . . . . . 62
4.3.2. Proofs for small gadgets . . . . . 63
4.3.3. Simulation-based proofs . . . . . 64
4.3.4. Limitations . . . . . 66
4.4. Robust probing model . . . . . 67
4.4.1. Formal definition . . . . . 67
4.4.2. Proofs for small gadgets . . . . . 68
4.4.3. Limitations . . . . . 69
4.5. Random probing model and noisy leakage model . . . . . 70
4.5.1. Formal definition of the noisy leakage model . . . . . 70
4.5.2. Limitations . . . . . 70
4.5.3. Reduction to the probing model . . . . . 71
4.5.4. Formal definition of the random probing model . . . . . 71
4.5.5. Proofs in the random probing model . . . . . 72
4.5.6. Extension to handle physical defaults . . . . . 73
4.6. Composition . . . . . 74
4.6.1. Composition in the probing model . . . . . 74
4.6.2. Composition in the random probing model . . . . . 77
4.7. Conclusion . . . . . 81
4.8. Notes and further references . . . . . 81
4.9. References . . . . . 81

**Chapter 5. Masking Verification** . . . . . 83
Abdul Rahman TALEB

5.1. Introduction . . . . . 83
5.2. General procedure . . . . . 84
5.3. `Verify`: verification mechanisms for a set of variables . . . . . 87
5.3.1. Distribution-based `Verify` . . . . . 87
5.3.2. Simulation-based `Verify` . . . . . 90
5.4. `Explore`: exploration mechanisms for all sets of variables . . . . . 97
5.4.1. Probing model . . . . . 98
5.4.2. Random probing model . . . . . 102
5.4.3. Handling physical defaults . . . . . 107
5.5. Conclusion . . . . . 108
5.6. Notes and further references . . . . . 109
5.7. Solution to Exercise 5.1 . . . . . 109
5.8. References . . . . . 111

**Part 2. Cryptographic Implementations** . . . . . 113

**Chapter 6. Hardware Acceleration of Cryptographic Algorithms** . . 115
Lejla BATINA, Pedro Maat COSTA MASSOLINO and Nele MENTENS

6.1. Introduction . . . . . 115

6.2. Hardware optimization of symmetric-key cryptography . . . . . . . . . 116
6.2.1. Hardware implementation of the AES S-box . . . . . . . . . . . . . 117
6.2.2. Composite field based implementation of the AES S-box . . . . . . 117
6.3. Modular arithmetic for hardware implementations . . . . . . . . . . . . 118
6.3.1. Montgomery's arithmetic . . . . . . . . . . . . . . . . . . . . . . . 119
6.3.2. Barret reduction . . . . . . . . . . . . . . . . . . . . . . . . . . . 120
6.3.3. Implementations using residue number system . . . . . . . . . . . . 122
6.4. RSA implementations . . . . . . . . . . . . . . . . . . . . . . . . . . 123
6.4.1. Previous works on RSA implementations . . . . . . . . . . . . . . . 123
6.4.2. ECC implementations over prime fields . . . . . . . . . . . . . . . . 124
6.5. Post-quantum cryptography . . . . . . . . . . . . . . . . . . . . . . . 125
6.6. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 126
6.7. Notes and further references . . . . . . . . . . . . . . . . . . . . . . . 127
6.8. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 128

**Chapter 7. Constant-Time Implementations** . . . . . . . . . . . . . . . . 133
Thomas PORNIN

7.1. What does constant-time mean? . . . . . . . . . . . . . . . . . . . . . 133
7.1.1. Timing attacks . . . . . . . . . . . . . . . . . . . . . . . . . . . . 133
7.1.2. Applicability and importance . . . . . . . . . . . . . . . . . . . . . 134
7.1.3. Example: rejection sampling . . . . . . . . . . . . . . . . . . . . . 135
7.2. Low-level issues . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 138
7.2.1. CPU execution pipeline . . . . . . . . . . . . . . . . . . . . . . . . 138
7.2.2. Variable time instructions . . . . . . . . . . . . . . . . . . . . . . . 140
7.2.3. Memory and caches . . . . . . . . . . . . . . . . . . . . . . . . . . 143
7.2.4. Jumps and jump prediction . . . . . . . . . . . . . . . . . . . . . . 145
7.3. Primitive implementation techniques . . . . . . . . . . . . . . . . . . 146
7.3.1. Compiler issues and Booleans . . . . . . . . . . . . . . . . . . . . . 146
7.3.2. Bitwise Boolean logic . . . . . . . . . . . . . . . . . . . . . . . . . 150
7.4. Constant-time algorithms . . . . . . . . . . . . . . . . . . . . . . . . . 163
7.4.1. Modular integers . . . . . . . . . . . . . . . . . . . . . . . . . . . . 163
7.4.2. Modular exponentiation . . . . . . . . . . . . . . . . . . . . . . . . 166
7.4.3. Modular inversion . . . . . . . . . . . . . . . . . . . . . . . . . . . 168
7.4.4. Elliptic curves . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 171
7.5. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 175

**Chapter 8. Protected AES Implementations** . . . . . . . . . . . . . . . . 177
Franck RONDEPIERRE

8.1. Generic countermeasures . . . . . . . . . . . . . . . . . . . . . . . . . 178
8.1.1. 1 among N . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 178
8.1.2. Integrity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 179
8.2. Secure evaluation of the SubByte function . . . . . . . . . . . . . . . . 180
8.2.1. S-box and inverse S-box . . . . . . . . . . . . . . . . . . . . . . . 181

8.2.2. Security . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 182
8.2.3. Secure table lookup . . . . . . . . . . . . . . . . . . . . . . . . . 183
8.2.4. Evaluation in $\mathbb{F}_{2^8}$ . . . . . . . . . . . . . . . . . . . . . . . . . . 184
8.2.5. Tower field . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 187
8.2.6. Bitslice S-box . . . . . . . . . . . . . . . . . . . . . . . . . . . . 188
8.2.7. How to select the S-box implementation . . . . . . . . . . . . . . 189
8.3. Other functions of AES . . . . . . . . . . . . . . . . . . . . . . . . . 192
8.3.1. State . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 192
8.3.2. ShiftRow . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 192
8.3.3. MixColumn . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 192
8.3.4. KeyScheduling . . . . . . . . . . . . . . . . . . . . . . . . . . . 193
8.3.5. AES inverse function . . . . . . . . . . . . . . . . . . . . . . . . 194
8.3.6. Key generation . . . . . . . . . . . . . . . . . . . . . . . . . . . 194
8.3.7. Interface . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 195
8.3.8. Bitsliced state example . . . . . . . . . . . . . . . . . . . . . . . 195
8.4. Notes and further references . . . . . . . . . . . . . . . . . . . . . . 197
8.5. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 198

**Chapter 9. Protected RSA Implementations** . . . . . . . . . . . . . . . . 201
Mylène ROUSSELLET, Yannick TEGLIA and David VIGILANT

9.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 201
9.1.1. The RSA cryptosystem . . . . . . . . . . . . . . . . . . . . . . . 201
9.1.2. RSA and security recommendations . . . . . . . . . . . . . . . . . 201
9.1.3. RSA-CRT and straightforward mode . . . . . . . . . . . . . . . . 202
9.1.4. Toward a device product embedding RSA-CRT . . . . . . . . . . . 203
9.2. Building a protected RSA implementation step by step . . . . . . . . . 203
9.2.1. Loading RSA-CRT key parameter – Step 1 . . . . . . . . . . . . . 204
9.2.2. Message reductions – Step 2 . . . . . . . . . . . . . . . . . . . . . 205
9.2.3. Exponentiations – Step 3 . . . . . . . . . . . . . . . . . . . . . . . 206
9.2.4. Recombination – Step 4 . . . . . . . . . . . . . . . . . . . . . . . 211
9.2.5. Return S . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 212
9.2.6. Protected RSA-CRT pseudo-code . . . . . . . . . . . . . . . . . . 212
9.3. Remarks and open discussion . . . . . . . . . . . . . . . . . . . . . . 213
9.3.1. Security resistance consideration . . . . . . . . . . . . . . . . . . 213
9.4. Notes and further references . . . . . . . . . . . . . . . . . . . . . . 214
9.5. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 220

**Chapter 10. Protected ECC Implementations** . . . . . . . . . . . . . . . 225
Łukasz CHMIELEWSKI and Louiza PAPACHRISTODOULOU

10.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 225
10.2. Protecting ECC implementations and countermeasures . . . . . . . . 226
10.2.1. Unified arithmetic and complete formulae . . . . . . . . . . . . . . 227
10.2.2. Constant-time scalar multiplication . . . . . . . . . . . . . . . . . 228

10.2.3. Elimination of if-statements even dummy ones . . . . . . . . . . . 230
10.2.4. Scalar randomization . . . . . . . . . . . . . . . . . . . . . . . . . . 234
10.2.5. Coordinate and point randomizations . . . . . . . . . . . . . . . . 236
10.2.6. Protection against address-bit side-channel attacks . . . . . . . . . 238
10.2.7. Additional fault injection protections . . . . . . . . . . . . . . . . 241
10.3. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 242
10.4. Notes and further references . . . . . . . . . . . . . . . . . . . . . 242
10.5. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 245

**Chapter 11. Post-Quantum Implementations** . . . . . . . . . . . . . . . 249
Matthias J. KANNWISCHER, Ruben NIEDERHAGEN,
Francisco RODRÍGUEZ-HENRÍQUEZ and Peter SCHWABE

11.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 249
11.2. Post-quantum encryption and key encapsulation . . . . . . . . . . . 251
11.2.1. Lattice-based KEMs – Kyber . . . . . . . . . . . . . . . . . . . . . 251
11.2.2. Code-based KEMs – Classic McEliece . . . . . . . . . . . . . . . 256
11.2.3. Isogeny-based KEMs . . . . . . . . . . . . . . . . . . . . . . . . . 259
11.2.4. IND-CCA2 security . . . . . . . . . . . . . . . . . . . . . . . . . . 263
11.3. Post-quantum signatures . . . . . . . . . . . . . . . . . . . . . . . . 265
11.3.1. Lattice-based signatures – Dilithium . . . . . . . . . . . . . . . . . 266
11.3.2. Multivariate-quadratic-based signatures – UOV . . . . . . . . . . 269
11.3.3. Hash-based signatures – XMSS and SPHINCS$^+$ . . . . . . . . . . 272
11.4. Notes and further references . . . . . . . . . . . . . . . . . . . . . 275
11.5. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 278

**Part 3. Hardware Security** . . . . . . . . . . . . . . . . . . . . . . . . 289

**Chapter 12. Hardware Reverse Engineering and Invasive Attacks** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 291
Sergei SKOROBOGATOV

12.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 291
12.2. Preparation for hardware attacks . . . . . . . . . . . . . . . . . . . 291
12.2.1. Preparation at PCB level . . . . . . . . . . . . . . . . . . . . . . . 292
12.2.2. Preparation at component level . . . . . . . . . . . . . . . . . . . 295
12.2.3. Preparation at silicon level . . . . . . . . . . . . . . . . . . . . . . 299
12.3. Probing attacks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 300
12.4. Delayering and reverse engineering . . . . . . . . . . . . . . . . . . 303
12.4.1. Chemical deprocessing . . . . . . . . . . . . . . . . . . . . . . . . 303
12.4.2. Mechanical deprocessing . . . . . . . . . . . . . . . . . . . . . . . 304
12.4.3. Chemical–mechanical polishing (CMP) deprocessing . . . . . . . 305
12.4.4. Plasma, RIE and FIB deprocessing . . . . . . . . . . . . . . . . . 305
12.4.5. Staining techniques . . . . . . . . . . . . . . . . . . . . . . . . . . 306
12.4.6. From images to netlist . . . . . . . . . . . . . . . . . . . . . . . . 307

12.5. Memory dump and hardware cloning . . . . . . . . . . . . . . . . . 309
12.6. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 311
12.7. Notes and further references . . . . . . . . . . . . . . . . . . . . . . . 311
12.8. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 312

**Chapter 13. Gate-Level Protection** . . . . . . . . . . . . . . . . . . . . . 315
Sylvain GUILLEY and Jean-Luc DANGER

13.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 315
13.2. DPL principle, built-in DFA resistance, and latent side-channel vulnerabilities . . . . . . . . . . . . . . . . . . . . . . . . . . 316
13.2.1. Information hiding rationale . . . . . . . . . . . . . . . . . . . . . 316
13.2.2. DPL built-in DFA resistance . . . . . . . . . . . . . . . . . . . . . 317
13.2.3. Vulnerabilities with respect to side-channel attacks . . . . . . . . 317
13.3. DPL families based on standard cells . . . . . . . . . . . . . . . . . . 318
13.3.1. WDDL . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 318
13.3.2. MDPL . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 319
13.3.3. DRSL . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 319
13.3.4. STTL . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 323
13.3.5. BCDL . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 323
13.3.6. WDDL variants . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 323
13.4. Technological specific DPL styles . . . . . . . . . . . . . . . . . . . . 328
13.4.1. Full custom optimizations . . . . . . . . . . . . . . . . . . . . . . . 328
13.4.2. Asynchronous logic . . . . . . . . . . . . . . . . . . . . . . . . . . 330
13.4.3. Reversible differential logic . . . . . . . . . . . . . . . . . . . . . 330
13.5. DPL styles comparison . . . . . . . . . . . . . . . . . . . . . . . . . . 331
13.6. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 331
13.7. Notes and further references . . . . . . . . . . . . . . . . . . . . . . . 332
13.8. References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 334

**Chapter 14. Physically Unclonable Functions** . . . . . . . . . . . . . . 339
Jean-Luc DANGER, Sylvain GUILLEY, Debdeep MUKHOPADHYAY and Ulrich RUHRMAIR

14.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 339
14.1.1. Principle . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 339
14.1.2. The twin nature of PUFs . . . . . . . . . . . . . . . . . . . . . . . 341
14.1.3. Properties . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 342
14.1.4. Two broad classification of PUFs . . . . . . . . . . . . . . . . . . 344
14.1.5. Necessity of enrollment . . . . . . . . . . . . . . . . . . . . . . . . 345
14.1.6. Use-cases . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 346
14.2. PUF architectures . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 347
14.2.1. Weak PUFs . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 347
14.2.2. Strong PUFs . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 350
14.2.3. Big picture of PUF architectures . . . . . . . . . . . . . . . . . . . 353

14.3. Reliability enhancement . . . . . 353
14.3.1. Use of error correcting codes . . . . . 354
14.3.2. Discarding unreliable bits . . . . . 356
14.3.3. Stochastic model of reliability . . . . . 357
14.4. Entropy assessment . . . . . 358
14.4.1. Stochastic model of the entropy . . . . . 358
14.4.2. Entropy loss due to helper data . . . . . 359
14.5. Resistance to attacks . . . . . 361
14.5.1. Non-invasive attacks . . . . . 361
14.5.2. Semi-invasive attacks . . . . . 363
14.5.3. Invasive attacks . . . . . 364
14.6. Characterizations . . . . . 364
14.6.1. Reliability–aging . . . . . 364
14.6.2. Machine learning attacks on challenge–response protocol . . . . . 365
14.7. Standardization . . . . . 365
14.7.1. International standards . . . . . 365
14.7.2. Standards requiring PUF . . . . . 366
14.8. Notes and further references . . . . . 366
14.9. References . . . . . 368

**List of Authors** . . . . . 375

**Index** . . . . . 379

**Summary of Volume 1** . . . . . 385

**Summary of Volume 3** . . . . . 393