Contents

Preface xi
Christina BOURA and María NAYA-PLASENCIA

Part 1. Design of Symmetric-key Algorithms 1

Chapter 1. Introduction to Design in Symmetric Cryptography . . . 3
Joan DAEMEN

1.1. Introduction 3
1.2. Cryptographic building blocks 3
1.2.1. The block cipher and its variants 4
1.3. Differentially uniform functions 5
1.4. Arbitrary-length schemes 5
1.4.1. Modes and constructions 6
1.4.2. Dedicated schemes 7
1.4.3. Modes and constructions versus primitives 7
1.5. Iterated (tweakable) block ciphers and permutations 8
1.5.1. Cryptanalysis and safety margin 8
1.5.2. Designing the round function of primitives 9
1.6. A short history 10
1.6.1. The data encryption standard 10
1.6.2. The block cipher FEAL 11
1.6.3. Differential and linear cryptanalysis 11
1.6.4. The block cipher IDEA 12
1.6.5. The advanced encryption standard 12
1.6.6. Cache attacks 13
1.6.7. KECCAK 14
1.6.8. Lightweight cryptography 15

1.7. Acknowledgments 15
1.8. References 15

Chapter 2. The Design of Stream Ciphers 21
Chaoyun LI and Bart PRENEEL

2.1. Introduction 21
2.1.1. What is a synchronous additive stream cipher? 21
2.1.2. Generic construction 23
2.1.3. Generic attacks 24
2.1.4. Open competitions 25
2.1.5. Standards 26
2.2. Constructions based on FSRs 27
2.2.1. LFSR-based constructions 27
2.2.2. NFSR-based constructions 28
2.3. Table-based constructions 29
2.4. Block ciphers and permutations in stream cipher mode 29
2.4.1. Block cipher modes OFB and CTR 30
2.4.2. Permutations in stream cipher mode 30
2.5. Authenticated encryption (AE) 31
2.5.1. Block ciphers and permutations in stream cipher modes 32
2.6. Emerging low-complexity stream ciphers 33
2.7. References 34

Chapter 3. Block Ciphers 39
Orr DUNKELMAN

3.1. General purpose block ciphers 41
3.1.1. Feistel block ciphers 42
3.1.2. Substitution permutation networks 43
3.2. Key schedule algorithms 44
3.3. Generic attacks 46
3.4. Tweakable block ciphers 48
3.5. Some positive results concerning security 49
3.6. The case of algebraic ciphers 51
3.7. References 53

Chapter 4. Hash Functions 55
Gilles VAN ASSCHE

4.1. Definitions and requirements 55
4.1.1. An ideal model: the random oracle 57
4.1.2. Expressing security claims 58
4.2. Design of hash functions 60
4.2.1. The Merkle-Damgård construction 60

4.2.2. Fixing the Merkle-Damgård construction 61
4.2.3. Building a compression function 62
4.2.4. Indifferentiability 64
4.2.5. The sponge construction 65
4.2.6. KECCAK, SHA-3 and beyond 67
4.3. Tree hashing 68
4.4. References 69

Chapter 5. Modes of Operation 73
Gaëtan LEURENT

5.1. Encryption schemes 73
5.1.1. Cipher block chaining 74
5.1.2. Counter mode 75
5.2. Message authentication codes 75
5.2.1. CBC-MAC 76
5.2.2. PMAC 77
5.2.3. Hash-based MACs 77
5.2.4. Wegman-Carter MACs and GMAC 78
5.3. Security of modes: generic attacks 78
5.3.1. The birthday bound 79
5.3.2. Generic attack against iterated MACs 79
5.3.3. Generic attack against Wegman-Carter MACs 80
5.3.4. Generic attack against CBC 80
5.3.5. Generic attack against CTR 80
5.3.6. Small block sizes 81
5.3.7. Misuse 81
5.3.8. Limitations of encryption 82
5.4. References 83

Chapter 6. Authenticated Encryption Schemes 87
Maria EICHLSEDER

6.1. Introduction 87
6.2. Security notions 88
6.3. Design strategies for authenticated encryption 89
6.3.1. Generic composition 91
6.3.2. Dedicated primitive-based designs 92
6.3.3. Fully dedicated designs 94
6.3.4. Standards and competitions 95
6.4. References 96

Chapter 7. MDS Matrices 99
Gaëtan LEURENT

7.1. Definition 99
7.1.1. Differential and linear properties 100
7.1.2. Near-MDS matrices 101
7.2. Constructions 101
7.3. Implementation cost 102
7.3.1. Optimizing the implementation of a matrix 103
7.3.2. Implementation of the inverse matrix 104
7.4. Construction of lightweight MDS matrices 104
7.4.1. Choice of the field or ring 105
7.4.2. MDS matrices with the lowest XOR count 105
7.4.3. Iterative MDS matrices 106
7.4.4. Involutory MDS matrices 107
7.5. References 108

Chapter 8. S-boxes 111
Christina BOURA

8.1. Important design criteria 113
8.1.1. Differential properties 113
8.1.2. Linear properties 115
8.1.3. Algebraic properties 116
8.1.4. Other properties 117
8.2. Popular S-boxes for different dimensions 117
8.2.1. S-boxes with an odd number of variables 118
8.2.2. 4-bit S-boxes 118
8.2.3. 8-bit S-boxes 119
8.3. Further reading 119
8.4. References 119

Chapter 9. Rationale, Backdoors and Trust 123
Léo PERRIN

9.1. Lifecycle of a cryptographic primitive 124
9.1.1. Design phase 124
9.1.2. Public cryptanalysis 125
9.1.3. Deployment? 125
9.1.4. The limits of this process 126
9.2. When a selection process fails 126
9.2.1. Under-engineered algorithms 127
9.2.2. Primitives with hidden properties 128
9.3. Can we trust modern algorithms? 131
9.3.1. Standardization and normalization 131

9.3.2. Some rules of thumb 132
9.4. References 133

Part 2. Security Proofs for Symmetric-key Algorithms 135

Chapter 10. Modeling Security 137
Bart MENNINK

10.1. Different types of adversary models 137
10.2. When is an attack considered successful? 138
10.3. Random oracle 138
10.4. Distinguishing advantage 139
10.5. Understanding the distinguishing advantage 141
10.5.1. Adversarial complexity 141
10.5.2. Claiming security 142
10.5.3. Breaking claims 143
10.6. Adaptation to block ciphers 143
10.6.1. Distinguishing advantage 144
10.6.2. Security of AES 145
10.7. Acknowledgments 146
10.8. References 146

Chapter 11. Encryption and Security of Counter Mode 147
Bart MENNINK

11.1. Block encryption 147
11.1.1. Padding 148
11.1.2. Cipher block chaining 149
11.2. Stream encryption 150
11.2.1. Output feedback mode 151
11.2.2. Counter mode 152
11.3. Provable security of modes: the case of counter mode 153
11.4. Acknowledgments 156
11.5. References 156

Chapter 12. Message Authentication and Authenticated Encryption 159
Tetsu IWATA

12.1. Message authentication 159
12.1.1. WCS construction 160
12.1.2. Provable security 161
12.2. Authenticated encryption 164
12.2.1. GCM, Galois/counter mode 164
12.2.2. Provable security 166

12.3. References 169

Chapter 13. H-coefficients Technique 171
Yannick SEURIN

13.1. The H-Coefficients technique 171
13.2. A worked out example: the three-round Feistel construction 176
13.3. The Even-Mansour construction 178
13.3.1. H-coefficients security proof 179
13.3.2. Extension to multiple rounds 181
13.4. References 182

Chapter 14. Chi-square Method 183
Mridul NANDI

14.1. Introduction 183
14.2. Preliminaries 185
14.2.1. PRF-security definition 185
14.2.2. Hypergeometric distribution 186
14.3. Truncation of random permutation 187
14.3.1. PRF-security of truncation 188
14.4. XOR of random permutations 190
14.5. Other applications of the chi-squared method 192
14.6. Acknowledgments 193
14.7. References 193

Part 3. Appendices 195

Appendix 1. Data Encryption Standard (DES) 197
Christina BOURA

Appendix 2. Advanced Encryption Standard (AES) 205
Christina BOURA and Orr DUNKELMAN

Appendix 3. PRESENT 217
Christina BOURA

Appendix 4. KECCAK 223
Christina BOURA

List of Authors 231

Index 233

Summary of Volume 2 239