

# Contents

<b>Preface</b> . . . . .	xiii
Christina BOURA and María NAYA-PLASENCIA	
<b>Part 1. Cryptanalysis of Symmetric-key Algorithms</b> . . . . .	1
<b>Chapter 1. Differential Cryptanalysis</b> . . . . .	3
Henri GILBERT and Jérémy JEAN	
1.1. Statistical attacks on block ciphers: preliminaries . . . . .	4
1.2. Principle of differential cryptanalysis and application to DES . . . . .	7
1.2.1. Differential transitions and differential characteristics . . . . .	7
1.2.2. Derivation of non-trivial differential characteristics . . . . .	10
1.2.3. Leveraging characteristics to mount a key-recovery attack . . . . .	14
1.3. Some refinements and generalizations . . . . .	18
1.3.1. Differential effect . . . . .	18
1.3.2. Truncated differentials . . . . .	19
1.4. Design strategies and evaluation . . . . .	20
1.4.1. Case of the <i>AES</i> . . . . .	21
1.4.2. Automated analysis . . . . .	23
1.5. Further notes and references . . . . .	23
1.6. References . . . . .	26
<b>Chapter 2. Linear Cryptanalysis</b> . . . . .	29
Kaisa NYBERG and Antonio FLÓREZ-GUTIÉRREZ	
2.1. History . . . . .	29
2.2. Correlation and linear hull . . . . .	30
2.3. Multidimensional linear approximation . . . . .	31

2.4. Walsh-Hadamard transform . . . . .	32
2.5. Linear approximation of an iterative block cipher . . . . .	32
2.6. Matsui's Algorithm 1 type of key recovery . . . . .	33
2.7. Matsui's Algorithm 2 type of key recovery . . . . .	34
2.8. Searching for linear approximations and estimating correlations . . . . .	35
2.9. Speeding up key recovery . . . . .	36
2.10. Key-recovery distinguisher . . . . .	38
2.11. Classical model of Algorithm 2 . . . . .	39
2.12. Algorithm 2 with distinct known plaintext and randomized key . . . . .	40
2.13. Multiple linear approximations . . . . .	40
2.14. Multidimensional linear cryptanalysis . . . . .	42
2.15. References . . . . .	43
<b>Chapter 3. Impossible Differential Cryptanalysis . . . . .</b>	<b>47</b>
Christina BOURA and María NAYA-PLASENCIA	
3.1. Finding impossible differentials . . . . .	48
3.2. Key recovery . . . . .	49
3.2.1. Data, time and memory complexities . . . . .	50
3.3. Some improvements . . . . .	52
3.3.1. Early abort technique . . . . .	52
3.3.2. Multiple impossible differentials or multiple extension paths . . . . .	53
3.4. Applications . . . . .	54
3.5. References . . . . .	54
<b>Chapter 4. Zero-Correlation Cryptanalysis . . . . .</b>	<b>57</b>
Vincent RIJMEN	
4.1. Correlation and linear cryptanalysis . . . . .	57
4.1.1. Correlation matrix . . . . .	57
4.1.2. Linear trails and linear hulls . . . . .	58
4.1.3. Approximations of linear functions . . . . .	59
4.1.4. Computing the correlations over a permutation . . . . .	60
4.2. Attacks using a linear hull with correlation zero . . . . .	60
4.2.1. Correlation zero in random permutations . . . . .	61
4.2.2. Distinguisher . . . . .	61
4.2.3. Reducing the data complexity . . . . .	62
4.3. Linear hulls with correlation zero . . . . .	62
4.3.1. Feistel ciphers . . . . .	63
4.3.2. AES . . . . .	64
4.3.3. Extended result on <i>AES</i> . . . . .	64
4.4. References . . . . .	64

---

<b>Chapter 5. Differential-Linear Cryptanalysis</b> . . . . .	67
Yosuke TODO	
5.1. Brief introduction of differential-linear attacks . . . . .	67
5.2. How to estimate correlations of a differential-linear distinguisher . . . .	69
5.3. On the key recovery . . . . .	71
5.4. State of the art for differential-linear attacks . . . . .	72
5.4.1. Differential-linear connecting table . . . . .	72
5.4.2. Three techniques to improve differential-linear attacks . . . . .	73
5.5. References . . . . .	76
<b>Chapter 6. Boomerang Cryptanalysis</b> . . . . .	77
Ling SONG	
6.1. Basic boomerang attack . . . . .	77
6.2. Variants and refinements . . . . .	79
6.3. Tricks and failures . . . . .	80
6.4. Formalize the dependency . . . . .	83
6.5. References . . . . .	86
<b>Chapter 7. Meet-in-the-Middle Cryptanalysis</b> . . . . .	89
Brice MINAUD	
7.1. Introduction . . . . .	89
7.2. Basic meet-in-the-middle framework . . . . .	90
7.2.1. The 2DES attack . . . . .	90
7.2.2. Algorithmic framework . . . . .	91
7.2.3. Complexity analysis and memory usage . . . . .	92
7.3. Meet-in-the-middle techniques . . . . .	94
7.3.1. Filtering . . . . .	94
7.3.2. Splice-and-cut . . . . .	96
7.3.3. Bicliques . . . . .	97
7.4. Automatic tools . . . . .	98
7.5. References . . . . .	98
<b>Chapter 8. Meet-in-the-Middle Demirci-Selçuk Cryptanalysis</b> . . . . .	101
Patrick DERBEZ	
8.1. Original Demirci-Selçuk attack . . . . .	101
8.2. Improvements . . . . .	103
8.2.1. Data/time/memory trade-off . . . . .	104
8.2.2. Difference instead of value . . . . .	104
8.2.3. Multiset . . . . .	105
8.2.4. Linear combinations . . . . .	105
8.2.5. Differential enumeration technique . . . . .	106

8.3. Finding the best attacks . . . . .	108
8.3.1. Tools . . . . .	108
8.3.2. Results . . . . .	109
8.4. References . . . . .	109
<b>Chapter 9. Invariant Cryptanalysis . . . . .</b>	<b>111</b>
Christof BEIERLE	
9.1. Introduction . . . . .	111
9.2. Invariants for permutations and block ciphers . . . . .	112
9.2.1. Invariant subspaces . . . . .	113
9.2.2. Quadratic invariants . . . . .	117
9.3. On design criteria to prevent attacks based on invariants . . . . .	117
9.4. A link to linear approximations . . . . .	119
9.5. References . . . . .	121
<b>Chapter 10. Higher Order Differentials, Integral Attacks and Variants . . . . .</b>	<b>123</b>
Anne CANTEAUT	
10.1. Integrals and higher order derivatives . . . . .	123
10.2. Algebraic degree of an iterated function . . . . .	126
10.3. Division property . . . . .	128
10.4. Attacks based on integrals . . . . .	130
10.4.1. Distinguishers . . . . .	130
10.4.2. Attacks . . . . .	130
10.5. References . . . . .	131
<b>Chapter 11. Cube Attacks and Distinguishers . . . . .</b>	<b>133</b>
Itai DINUR	
11.1. Cube attacks and cube testers . . . . .	133
11.1.1. Terminology . . . . .	134
11.1.2. Main observation . . . . .	135
11.1.3. The basic cube attack . . . . .	136
11.1.4. The preprocessing phase on cube attacks . . . . .	137
11.1.5. Cube testers . . . . .	138
11.1.6. Applications . . . . .	139
11.2. Conditional differential attacks and dynamic cube attacks . . . . .	140
11.2.1. Conditional differential attacks . . . . .	140
11.2.2. Dynamic cube attacks . . . . .	140
11.2.3. A toy example . . . . .	140
11.3. References . . . . .	141

<b>Chapter 12. Correlation Attacks on Stream Ciphers</b> . . . . .	143
Thomas JOHANSSON	
12.1. Correlation attacks on the nonlinear combination generator . . . . .	144
12.2. Correlation attacks and decoding linear codes . . . . .	145
12.3. Fast correlation attacks . . . . .	146
12.3.1. Fast correlation attacks and low weight feedback polynomials . . . . .	147
12.3.2. Finding low weight multiples of the feedback polynomial . . . . .	148
12.3.3. Fast correlation attacks by reducing the code dimension . . . . .	150
12.4. Generalizing fast correlation attacks . . . . .	151
12.4.1. The <i>E0</i> stream cipher . . . . .	151
12.4.2. The <i>A5/I</i> stream cipher . . . . .	152
12.5. References . . . . .	153
<b>Chapter 13. Addition, Rotation, XOR</b> . . . . .	155
Léo PERRIN	
13.1. What is ARX? . . . . .	155
13.1.1. Structure of an ARX-based primitive . . . . .	156
13.1.2. Development of ARX . . . . .	156
13.2. Understanding modular addition . . . . .	157
13.2.1. Expressing modular addition in $\mathbb{F}_2^n$ . . . . .	158
13.2.2. Cryptographic properties of modular addition . . . . .	158
13.3. Analyzing ARX-based primitives . . . . .	160
13.3.1. Searching for differential and linear trails . . . . .	160
13.3.2. Proving security against differential and linear attacks . . . . .	161
13.3.3. Other cryptanalysis techniques . . . . .	162
13.4. References . . . . .	163
<b>Chapter 14. SHA-3 Contest Related Cryptanalysis</b> . . . . .	167
Yu SASAKI	
14.1. Chapter overview . . . . .	167
14.2. Differences between attacks against keyed and keyless primitives . . . . .	168
14.3. Rebound attack . . . . .	169
14.3.1. Basic strategy of the rebound attack . . . . .	169
14.3.2. Rebound attack against AES-like structures . . . . .	171
14.4. Improving rebound attacks with Super-Sbox . . . . .	173
14.5. References for further reading about rebound attacks . . . . .	175
14.6. Brief introduction of other cryptanalysis . . . . .	176
14.6.1. Internal differential cryptanalysis . . . . .	176
14.6.2. Rotational cryptanalysis . . . . .	177
14.7. References . . . . .	177

<b>Chapter 15. Cryptanalysis of SHA-1</b> . . . . .	181
Marc STEVENS	
15.1. Design of SHA-1 . . . . .	181
15.2. SHA-1 compression function . . . . .	182
15.3. Differential analysis . . . . .	184
15.4. Near-collision attacks . . . . .	184
15.5. Near-collision search . . . . .	185
15.6. Message expansion differences . . . . .	186
15.7. Differential trail . . . . .	187
15.8. Local collisions . . . . .	187
15.9. Disturbance vector . . . . .	188
15.10. Disturbance vector selection . . . . .	189
15.11. Differential trail construction . . . . .	190
15.12. Message modification techniques . . . . .	190
15.13. Overview of published collision attacks . . . . .	191
15.14. References . . . . .	192
<b>Part 2. Future Directions</b> . . . . .	195
<b>Chapter 16. Lightweight Cryptography</b> . . . . .	197
Meltem SÖNMEZ TURAN	
16.1. Lightweight cryptography standardization efforts . . . . .	197
16.2. Desired features . . . . .	198
16.3. Design approaches in lightweight cryptography . . . . .	200
16.4. References . . . . .	202
<b>Chapter 17. Post-Quantum Symmetric Cryptography</b> . . . . .	203
María NAYA-PLASENCIA	
17.1. Different considered models . . . . .	204
17.1.1. With respect to the queries . . . . .	204
17.1.2. With respect to memory . . . . .	205
17.2. On Simon's and Q2 attacks . . . . .	206
17.2.1. Off-line Simon's attack . . . . .	207
17.3. Quantizing classical attacks in Q1 . . . . .	207
17.3.1. About collisions . . . . .	207
17.4. On the design of quantum-safe primitives . . . . .	208
17.5. Perspectives and conclusion . . . . .	209
17.5.1. About losing the quantum and classical surname . . . . .	209
17.5.2. No panic . . . . .	209
17.6. References . . . . .	209

---

<b>Chapter 18. New Fields in Symmetric Cryptography</b> . . . . .	215
Léo PERRIN	
18.1. Arithmetization-oriented symmetric primitives (ZK proof systems) . .	216
18.1.1. The current understanding of this new language . . . . .	217
18.1.2. The first attempts . . . . .	218
18.1.3. Cryptanalysis . . . . .	219
18.2. Symmetric ciphers for hybrid homomorphic encryption . . . . .	220
18.2.1. The current understanding of this new language . . . . .	221
18.2.2. First design strategies . . . . .	221
18.3. Parting thoughts . . . . .	223
18.4. References . . . . .	223
<b>Chapter 19. Deck-function-based Cryptography</b> . . . . .	227
Joan DAEMEN	
19.1. Block-cipher centric cryptography . . . . .	227
19.2. Permutation-based cryptography . . . . .	227
19.3. The problem of the random permutation security model . . . . .	228
19.4. Deck functions . . . . .	228
19.5. Modes of deck functions and instances . . . . .	229
19.6. References . . . . .	230
<b>List of Authors</b> . . . . .	231
<b>Index</b> . . . . .	233
<b>Summary of Volume 1</b> . . . . .	239