COMPUTER SCIENCE

Cryptography, Data Security

Symmetric Cryptography 2

Cryptanalysis and Future Directions

Coordinated by
Christina Boura
María Naya-Plasencia

ISTE

WILEY

Symmetric Cryptography 2

SCIENCES

Computer Science, Field Directors –
Valérie Berthé and Jean-Charles Pomerol

Cryptography, Data Security, Subject Head – Damien Vergnaud

Symmetric Cryptography 2

Cryptanalysis and Future Directions

Coordinated by
Christina Boura
María Naya-Plasencia

ISTE

WILEY

First published 2023 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2023930938

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-78945-147-4

ERC code:
PE6 Computer Science and Informatics
PE6_5 Cryptology, security, privacy, quantum cryptography

Contents

Preface xiii
Christina BOURA and María NAYA-PLASENCIA

Part 1. Cryptanalysis of Symmetric-key Algorithms 1

Chapter 1. Differential Cryptanalysis 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 *AES* 21
1.4.2. Automated analysis 23
1.5. Further notes and references 23
1.6. References 26

Chapter 2. Linear Cryptanalysis 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

Chapter 3. Impossible Differential Cryptanalysis 47
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

Chapter 4. Zero-Correlation Cryptanalysis 57
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 *AES* 64
4.4. References 64

Chapter 5. Differential-Linear Cryptanalysis 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

Chapter 6. Boomerang Cryptanalysis 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

Chapter 7. Meet-in-the-Middle Cryptanalysis 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

Chapter 8. Meet-in-the-Middle Demirci-Selçuk Cryptanalysis 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

Chapter 9. Invariant Cryptanalysis 111
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

Chapter 10. Higher Order Differentials, Integral Attacks and Variants 123
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

Chapter 11. Cube Attacks and Distinguishers 133
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

Chapter 12. Correlation Attacks on Stream Ciphers 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 *E0* stream cipher 151
12.4.2. The *A5/1* stream cipher 152
12.5. References 153

Chapter 13. Addition, Rotation, XOR 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

Chapter 14. SHA-3 Contest Related Cryptanalysis 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

Chapter 15. Cryptanalysis of SHA-1 181
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

Part 2. Future Directions 195

Chapter 16. Lightweight Cryptography 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

Chapter 17. Post-Quantum Symmetric Cryptography 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

Chapter 18. New Fields in Symmetric Cryptography 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

Chapter 19. Deck-function-based Cryptography 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

List of Authors 231

Index 233

Summary of Volume 1 239

Preface

Christina BOURA[1] and María NAYA-PLASENCIA[2]
[1] *University of Paris-Saclay, UVSQ, CNRS, Versailles, France*
[2] *Inria, Paris, France*

Symmetric-key cryptology is one of the two main branches of modern cryptology. It comprises all primitives, modes and constructions used to ensure the confidentiality, authenticity and integrity of communications by means of a single key shared between the two communicating parties. Hash functions and some other keyless constructions are equally considered as symmetric constructions because of the similarity in the design and analysis with classical keyed symmetric ciphers. Symmetric algorithms are essential for establishing secure communications, as they can have very compact implementations and achieve high speed in both software and hardware. Furthermore, compared to public-key algorithms, keys used in symmetric cryptography are short, typically of 128 or 256 bits only.

The goal of this two-volume project is to provide a thorough overview of the most important design, cryptanalysis and proof techniques for symmetric designs. The first volume is dedicated to the most popular design trends for symmetric primitives, modes and constructions, and to the presentation of the most important proof techniques. On the other hand, the current volume describes and analyzes some of the most well-established and powerful cryptanalysis techniques against symmetric constructions.

Cryptanalysis is an essential process for establishing trust toward the symmetric ciphers to be used and deployed. Indeed, in symmetric cryptography, it is common to provide security proofs for the modes of operation and high-level constructions. These security proofs, analyzed in Volume 1, are fundamental for having confidence in the high-level constructions themselves, but they often rely on unrealistic assumptions, for example, by considering the internal functions to be perfect random ones. Therefore, in order to trust the primitives, cryptanalysis is a necessary process to be taken into account together with the security proofs.

Symmetric Cryptography 2,
coordinated by Christina BOURA and María NAYA-PLASENCIA.

The first modern symmetric cryptanalysis techniques started developing almost together with the appearance of the first symmetric designs. These first cryptanalysis techniques have not stopped evolving since. Moreover, the appearance of new designs had as a consequence the development of new analysis techniques adapted to these new schemes.

The goal of this second volume is to present the most powerful and the most promising attacks among those that have emerged since the 1980s. The book is divided into two parts. The first part contains 15 chapters and gives an overview of the most important cryptanalysis techniques. The second part is composed of four chapters and investigates some future directions for the field of symmetric cryptology.

Chapter 1 is dedicated to differential cryptanalysis, the oldest and probably the most well-studied attack against block ciphers and related primitives. First, a general background for statistical attacks is provided and the notion of distinguisher is introduced. Then, the most important notions encountered in differential cryptanalysis are given. Some possible refinements and extensions of the basic attack are provided, notably the differential effect and truncated differential characteristics. Finally, the most prominent design approaches to achieve resistance against this class of attacks are given.

Together with differential cryptanalysis, linear cryptanalysis is without doubt the second most well-known analysis technique against block ciphers. This technique is described in Chapter 2. After a brief historical note, the main notions for this attack, notably those of correlation, linear hull and multidimensional linear approximations are presented. Then, two well-known algorithms for key recovery, namely Matsui's algorithms 1 and 2, are given. The problem of finding good linear approximations for a given cipher is analyzed next and some techniques to speed up key recovery are given. Finally, two extensions of classical linear cryptanalysis are provided: the use of multiple linear approximations and the technique of multidimensional linear cryptanalysis.

Impossible differential cryptanalysis is another powerful attack against block ciphers. The idea, explained in Chapter 3, is to exploit differentials of probability zero. The distinguishing part, consisting of finding good impossible differentials, is first analyzed. Techniques for the key recovery part are given next. In this part, closed formulas for estimating the complexity of an attack are given. Some improvements to the classical version of this cryptanalysis technique are provided at the end of this chapter.

Zero-correlation attacks are an extension of linear cryptanalysis. These attacks, presented in Chapter 4, are based on linear approximations with correlation exactly zero. First, this chapter presents the central notion of correlation matrices. The

notions of linear trails and hulls are defined once again and some results on computing the correlations over a permutation are provided next. Then, this chapter analyzes how linear hulls with correlation zero can be used to mount an attack and techniques for reducing the data complexity are given. Finally, some important applications for Feistel ciphers and for the advanced encryption standard (AES) are discussed.

Chapter 5 is dedicated to differential-linear attacks. This cryptanalysis technique consists of successfully combining a differential attack together with a linear one. First, the attack framework is presented and ways to estimate correlations of a differential-linear distinguisher are given next. Then, the key recovery part is discussed and the notion of differential-linear connecting table (DLCT) is presented. At the end, three techniques to improve differential-linear attacks are discussed.

Boomerang attacks are statistical attacks against block ciphers based on differential cryptanalysis. Chapter 6 introduces this type of cryptanalysis and some of its refinements, namely, the amplified boomerang and rectangle attacks. A discussion on the probability computation of boomerangs is next given, and several ways to improve or formalize this computation are discussed. Finally, a recent tool to calculate the boomerang probability for a single S-box, called Boomerang connectivity table (BCT) is presented together with its Feistel variant, FBCT.

Chapter 7 gives an overview of another famous cryptanalysis technique called meet-in-the-middle cryptanalysis. Meet-in-the-middle attacks are among the oldest symmetric cryptanalysis techniques and still continue to evolve. This chapter starts by presenting the basic meet-in-the-middle framework together with a first complexity analysis. The most important techniques used in modern meet-in-the-middle cryptanalysis are given next, such as the partial or indirect matching, the sieve-in-the-middle or the slice-and-cut technique. Finally, a method called biclique, which permits extension of the number of rounds of a meet-in-the-middle attack, is presented.

Chapter 8 presents meet-in-the-middle Demirci-Selçuk attacks, an advanced form of meet-in-the-middle cryptanalysis, particularly successful on reduced versions of the AES. The chapter starts by presenting the basic form of this attack and discusses its application to the AES. Then, several refinements and techniques are given. A discussion of how to choose the best parameters for mounting such an attack is provided, and finally a series of tools for applying a meet-in-the-middle attack in an automated way are briefly presented.

Invariant attacks are a form of structural cryptanalysis against block ciphers and cryptographic permutations that showed to be particularly efficient against some lightweight cryptographic designs. Chapter 9 presents the most important concepts and ideas behind two important invariant attacks classes, the invariant subspace

attacks and the nonlinear invariant attacks. Methods to detect potential vulnerabilities in cryptographic designs that could lead to the presence of invariants are discussed. Finally, design criteria to prevent attacks based on invariants are provided, and a link between invariant attacks and linear approximations is discussed.

Chapter 10 gives an overview of higher order differential and integral attacks as well as some of their most important variants. All these attacks exploit either some algebraic or some structural property of the underlying design, or sometimes both type of properties at the same time. The chapter starts by describing the notions of integrals and higher order derivatives. The notion of algebraic degree, essential for these attacks, and its properties for iterated permutations are presented next. A powerful tool, called the division property, that can be seen as a combination of integral and higher order differential cryptanalysis is given. Finally, attacks based on integrals are discussed.

Cube attacks and cube testers are additional methods of algebraic cryptanalysis that target designs with a relatively low number of nonlinear operations. Chapter 11 is dedicated to this class of attacks and summarizes the main ideas of these techniques. The classical cube attack that aims at recovering the secret key by analyzing the algebraic form of the cipher is described first. Then, a related distinguishing technique, called cube testers, is presented. Finally, conditional differential attacks and dynamic cube attacks, key recovery techniques related to cube attacks, are briefly given.

Chapter 12 describes correlation attacks against stream ciphers, one of the most well-studied and efficient cryptanalysis technique against this class of algorithms. The main idea of attacks against nonlinear combination generators is first presented. The link between correlation attacks and the linear codes decoding problem is next presented. Notably, the so-called fast correlation attacks that are attacks exploiting the above link to speed up the decoding problem are extensively analyzed. Finally, the chapter is concluded with two generalizations of correlation attacks on the stream ciphers E0 and A5/1.

ARX ciphers are constructions that only use the operations of modular addition, rotation and XOR to compute their output. These ciphers, described in Chapter 13, permit constant-time and extremely fast implementations in software and have been used in several popular designs and standards. The basic structure of such schemes is first described. Then, the development of ARX ciphers since the 1980s until today is provided. The properties of modular addition, the only nonlinear operation in these constructions, are discussed next as these properties are crucial for understanding the security of these schemes. Finally, methods and tools for analyzing the security of ARX ciphers are presented.

The NIST SHA-3 competition was a public competition held by the US National Institute of Standards and Technology (NIST) between 2008 and 2012. Its goal was

to develop and standardize a new hash function called SHA-3. During the 4 years of the competition, many new hash function cryptanalysis techniques emerged. Chapter 14 is dedicated to the presentation of some of these techniques. First, a discussion of the difference between attacks against keyed and keyless primitives is provided. Then, the biggest part of this chapter is dedicated to the description of the rebound attack, probably the most powerful technique that emerged in this context against substitution-permutation network (SPN)-based hash functions. At the end of this chapter, other new cryptanalysis methods developed against some SHA-3 candidates, notably the internal differential and the rotation cryptanalysis, are presented.

SHA-1 is a standardized cryptographic hash function, deprecated since 2011, but that was implemented inside a multitude of industrial products for decades and is still in use in many applications. The cryptanalysis efforts against this standard form a fascinating series of results until the practical break of the function in 2017. Chapter 15 is dedicated to the cryptanalysis of SHA-1 and describes the most important cryptanalysis techniques that were developed while trying to break SHA-1.

The second part of this book is consecrated to the discussion of some promising future directions for the field of symmetric cryptology.

During the last decade, many resource-constrained computing environments were developed and largely deployed. Most of them treat sensitive data and need to implement cryptographic algorithms to ensure their security. However, most of the general-purpose cryptographic algorithms cannot be implemented on such constrained devices while keeping decent performances, thus new cryptographic constructions are needed. Lightweight cryptography encompasses all cryptographic primitives, schemes and protocols that are optimized for resource-constrained devices. Chapter 16 is dedicated to lightweight cryptography and provides an overview of the standardization efforts, desired features and design trends for these applications. The NIST standardization process for lightweight cryptography, a public competition launched in 2018, is notably discussed.

The future arrival of quantum computers will have enormous consequences for the field of cryptography. The cryptographic community has been devoting significant time and effort over several years in anticipation of these potential effects. We know today that the most deployed public key schemes will be broken, because notably of Shor's algorithm, and for this reason the public key community is actively searching for solutions and replacements. However, for symmetric algorithms, the situation is different. The main quantum algorithm relevant to symmetric cryptography is Grover's algorithm that permits to accelerate the generic exhaustive search attack by a square root. Thus, doubling the size of the key would potentially be sufficient to overcome this problem. However, it is naïve to believe that this will be the only consequence for symmetric schemes. For this reason, for some years, a

new domain dedicated to the quantum cryptanalysis of symmetric primitives, modes and constructions emerged. The most important of these efforts and the latest results are described in Chapter 17 of this book.

Not all symmetric algorithms are intended to be run on classical computing environments such as CPUs or smartcards. Chapter 18 describes the last efforts made in designing the newly introduced arithmetization-oriented (AO) symmetric ciphers, intended to be used within some particular zero-knowledge protocols, homomorphic encryption (HE) or multi-party computation (MPC) schemes. This chapter describes the most important design strategies for this family of ciphers and briefly discusses the most promising cryptanalysis techniques against them.

Chapter 19 describes finally some promising future directions for the design of symmetric primitives. In particular, doubly extendable cryptographic keyed (deck) functions are discussed.

The field of cryptography has never stopped evolving since the appearance of the first commercial cryptographic applications in the 1970s. Due to this constant evolution, providing a complete survey of all the design trends, cryptanalysis techniques or proof methods is an extremely difficult task. We believe, however, that this book offers a good starting point to all readers interested in learning about the most important and promising results of the field, in particularly to all those wishing to learn how to design and analyze a secure symmetric cipher. We believe that the two volumes of this work will be helpful to researchers, master's and PhD students studying or working in the field of cryptography as well as to all professionals working in the field of cybersecurity.

July 2023