Department of Information and Computer Science

Studies in Lightweight Cryptography

Hadi Soleimany

Aalto University

DOCTORAL DISSERTATIONS

Aalto University publication series
DOCTORAL DISSERTATIONS 211/2014

Studies in Lightweight Cryptography

Hadi Soleimany

A doctoral dissertation completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Science, at a public examination held at the lecture hall T2 of the school on 30 January 2015 at 12.

Aalto University
School of Science
Department of Information and Computer Science

Supervising professor
Prof. Kaisa Nyberg

Preliminary examiners
Prof. Lars R. Knudsen, Technical University of Denmark, Denmark
Prof. Carlos Cid, Royal Holloway, University of London, United Kingdom

Opponents
Prof. Carlos Cid, Royal Holloway, University of London, United Kingdom
Assist. Prof. Andrey Bogdanov, Technical University of Denmark, Denmark

Aalto University publication series
DOCTORAL DISSERTATIONS 211/2014

ISBN 978-952-60-6025-5 (printed)
ISBN 978-952-60-6026-2 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-60-6026-2

Unigrafia Oy
Helsinki 2014

Finland

Aalto University

Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

Author
Hadi Soleimany

Name of the doctoral dissertation
Studies in Lightweight Cryptography

Publisher School of Science

Unit Department of Information and Computer Science

Series Aalto University publication series DOCTORAL DISSERTATIONS 211/2014

Field of research Theoretical Computer Science

Manuscript submitted 26 September 2014 **Date of the defence** 30 January 2015

Permission to publish granted (date) 28 November 2014 **Language** English

□ **Monograph** ☒ **Article dissertation (summary + original articles)**

Abstract

The decreasing size of devices is one of the most significant changes in telecommunication and information technologies. This change has been accompanied by a dramatic reduction in the cost of computing devices. The dawning era of ubiquitous computing has opened the door to extensive new applications. Ubiquitous computing has found its way into products thanks to the improvements in the underlying enabling technologies. Considerable developments in constraint devices such as RFID tags facilitate novel services and bring embedded computing devices to our everyday environments. The changes that lie ahead will eventually make pervasive computing devices an integral part of our world.

The growing prevalence of pervasive computing devices has created a significant need for the consideration of security issues. However, security cannot be considered independently, but instead, should be evaluated alongside related issues such as performance and cost. In particular, there are several limitations facing the design of appropriate ciphers for extremely constrained environments. In response to this challenge, several lightweight ciphers have been designed during the last years. The purpose of this dissertation is to evaluate the security of the emerging lightweight block ciphers.

This dissertation develops cryptanalytic methods for determining the exact security level of some inventive and unconventional lightweight block ciphers. The work studies zero-correlation linear cryptanalysis by introducing the Matrix method to facilitate the finding of zero-correlation linear approximations. As applications, we perform zero-correlation cryptanalysis on the 22-round LBlock and TWINE. We also perform simulations on a small variant of LBlock and present the first experimental results to support the theoretical model of the multidimensional zero-correlation linear cryptanalysis method. In addition, we provide a new perspective on slide cryptanalysis and reflection cryptanalysis by extending previous research of self-similarity cryptanalysis. Unlike classical techniques, our approach is not limited to deterministic characteristics. To demonstrate the impact of our model we provide statistical and structural analysis of three well-known lightweight block ciphers: ITUbee, Zorro and LED. As a result of the analysis presented in this work new security criteria for PRINCE-like ciphers are obtained.

Keywords block cipher, lightweight cryptography, zero-correlation linear cryptanalysis, self-similarity cryptanalysis, slide cryptanalysis, reflection cryptanalysis

ISBN (printed) 978-952-60-6025-5 **ISBN (pdf)** 978-952-60-6026-2

ISSN-L 1799-4934 **ISSN (printed)** 1799-4934 **ISSN (pdf)** 1799-4942

Location of publisher Helsinki **Location of printing** Helsinki **Year** 2014

Pages 157 **urn** http://urn.fi/URN:ISBN:978-952-60-6026-2

Aalto-yliopisto

Tiivistelmä

Aalto-yliopisto, PL 11000, 00076 Aalto www.aalto.fi

Tekijä
Hadi Soleimany

Väitöskirjan nimi
Tutkimuksia kevyen luokan salaustekniikasta

Julkaisija Perustieteiden korkeakoulu

Yksikkö Tietojenkäsittelytieteen laitos

Sarja Aalto University publication series DOCTORAL DISSERTATIONS 211/2014

Tutkimusala Tietojenkäsittelyteoria

Käsikirjoituksen pvm 26.09.2014 **Väitöspäivä** 30.01.2015

Julkaisuluvan myöntämispäivä 28.11.2014 **Kieli** Englanti

□ **Monografia** ☒ **Yhdistelmäväitöskirja (yhteenveto-osa + erillisartikkelit)**

Tiivistelmä

Informaatio- ja tietoliikennetekniikan merkittävimpiä muutoksia on ollut siirtyminen yhä pienempiin ja pienempiin laitteisiin, joka on myös alentanut niiden hintoja. Ubiikkilaskennan aikakauden koittaessa ovet avautuvat myös laajamittaisiin uusiin sovelluksiin. Ubiikkilaskenta on löytänyt tiensä tuotteisiin sen vaatimissa teknologioissa tapahtuneiden parannusten ansiosta. Rajoitteisten laitteiden kuten RFID-tagien kehittyminen mahdollistaa uusia palveluja ja tuo sulautetut järjestelmät jokapäiväiseen toimintaympäristöömme. Kaikkialle leviävät langattomat laitteet tulevat kiinteäksi osaksi maailmaamme.

Kaikkialle läpitunkevan laskennan lisääntyessä turvallisuusnäkökohtien ottaminen huomioon on entistä tärkeämpää. Turvallisuutta ei kuitenkaan voi tarkastella irrallaan muusta kokonaisuudesta, vaan sitä tulee arvioida suhteessa muihin ominaisuuksiin kuten suorituskykyyn ja kustannuksiin. Erityisesti kun suunnitellaan salausteknisiä algoritmeja äärimmäisen rajoitteisiin ympäristöihin kohdataan useita haasteita joihin on viime vuosina pyritty vastaamaan esittämällä lukuisia uusia kevyen luokan salausalgoritmeja. Tämän väitöskirjatyön tarkoituksena on arvioida uusien kevyen luokan salausalgoritmien kryptografista turvallisuutta.

Väitöskirjassa kehitetään kryptoanalyyttisiä menetelmiä, joilla voidaan määrittää eräiden uraa uurtavien uusien kevyen luokan lohkosalausalgoritmien turvallisuustaso. Työssä tutkitaan lineaarista nollakorrelaatiomenetelmää ja esitetään matriisimenetelmä, jolla voidaan helpottaa nollakorrelaatiorelaatioiden löytämistä. Sovelluksena esitetään 22 kierroksen LBlock ja TWINE lohkosalausalgoritmien nollakorrelaatioanalyysi. Analyysimenetelmää myös simuloidaan LBlock-algoritmin pienennetyllä versiolla. Tuloksena on ensimmäinen tilastolliselle nollakorrelaatiomenetelmälle suoritettu kokeellinen analyysi ja se tukee aiemmin esitettyä teoreettista mallia. Tutkimuksessa saavutetaan myös uusia tuloksia lohkosalausalgoritmien liukuanalyysi- ja heijastusanalyysimenetelmistä, jotka laajentavat merkittävästi aikaisemmin tunnettujen lohkosalausalgoritmien nk. itseensärinnastavien menetelmien hyödynnettävyyttä ja toimivuutta. Päinvastoin kuin klassiset lähestymistavat, tässä työssä esitetyt laajennukset eivät rajoitu vain deterministisen relaation tapaukseen. Uuden mallin toimivuutta havainnollistetaan esittämällä uusia tilastollisia ja rakenteellisia kryptoanalyyseja tunnetuille kevyen luokan lohkosalausalgoritmeille: ITUBee, Zorro ja LED. Heijastusmenetelmällä suoritetun analyysin pohjalta esitetään myös uusia suunnittelukriteerejä PRINCE-tyypin salausalgoritmeille.

Avainsanat Lohkosalausalgoritmi, kevyen luokan salaustekniikka, lineaarinen nollakorrelaatiomenetelmä, itseensä rinnastavat kryptoanalyysimenetelmät, liukumenetelmä, heijastusmenetelmä

ISBN (painettu) 978-952-60-6025-5 **ISBN (pdf)** 978-952-60-6026-2

ISSN-L 1799-4934 **ISSN (painettu)** 1799-4934 **ISSN (pdf)** 1799-4942

Julkaisupaikka Helsinki **Painopaikka** Helsinki **Vuosi** 2014

Sivumäärä 157 **urn** http://urn.fi/URN:ISBN:978-952-60-6026-2

Preface

This dissertation is a result of the research that has been carried out during the last three years at the Department of Information and Computer Science, Aalto University School of Science. This work has been funded by the Helsinki Doctoral Programme in Computer Science - Advanced Computing and Intelligent Systems and partially by the European Commission through the ICT program under contract ICT-2007-216676 ECRYPT II. Also a personal grant awarded by the Nokia Foundation is gratefully acknowledged.

First and foremost, I must praise and thank God for uncountable blessings which He has bestowed upon me throughout my life. These blessings have made me who I am today.

I would like to extend my deep gratitude to all the people who have supported me during the last years, and this thesis would not have been as successful without them.

I would like to express my deep gratitude to my supervisor Prof. Kaisa Nyberg for giving me such a wonderful opportunity to do my Ph.D. at her group. Her constant support, excellent guidance and useful feedbacks made this work possible. I especially would like to acknowledge Kaisa for her endless patience during our insightful discussions. *"Kiitos Paljon Kaisa!"*

Next, I would like to express my gratitude to all members (former and current) of our cryptography group for their help and their friendship: Céline Blondeau, Billy Brumley, Risto Hakala, Kimmo Järvinen, Mohsin Khan, Alexander Kaitai Liang and Léo Perrin. In particular, I would like to thank Céline from whom I learned a lot during our fruitful collaboration. *"Merci Beaucoup!"* Special thanks go to Kimmo and Risto, not only for using their knowledge, but also for providing useful information for my everyday life in Finland. *"Kiitos Risto ja Kimmo"*.

I thank my pre-examiners, Prof. Lars R. Knudsen and Prof. Carlos Cid for taking their time to review my thesis and for their comments. I am grateful to Prof. Carlos Cid and Prof. Andrey Bogdanov for the honor of having them as the opponents.

I wish to thank my friends with whom I have shared wonderful moments during the last years. In particular, I thank Shemshir Abbas, Mohammad Albooye, Heidar Alhelo, Somaya Arian, Abbas Bahmanpour, Hossein Bahmanpour, Majid Bahmanpour, Fahim Hasan, Yahya Afshar, Afshin Hasani, Mahdi Hashemi, Paula Kemell, Ehsan Khoramshahi, Mahdi Khosravi, Hossein Mahdavi, Salman Malekia, Mohammad Moshtari, Furqan Reza, Mudasser Sabir, Maryam Pahlevan, Sorush Salmani, Reza Sadeghi, as well as their family. I will never forget how important your friendship has been to me during my stay in Finland. *“Mamnun, Bahut Shukria, Shokran Jazila, Kiitos”*.

Last but by no means the least, I would like to take this opportunity to thank my family. I heartily thank my parents although no words can express my gratitude to them. My father always supported me with his excellent advices and helpful consultations. My lovely mother has a great role in my life by her devotion. *“Khazeaane Dastane Mehrbanetan Ra Mibusam”*. I am very thankful to my sister and brother as well as their spouses for making our home so warm and loving. I also would like to thank my parents-in-law for their endless help. Finally, I heartily thank my wife for everything! An incredible seven years has passed since our marriage, and I have seen from her JUST honesty, love and patience. *“Mamnun be Khatere Sedaghat, Mohabbatha va Sabre Bipayan”*.

Espoo, December 2, 2014,

Hadi Soleimany

Contents

List of Publications

This thesis consists of an overview and of the following publications which are referred to in the text by their Roman numerals.

I Hadi Soleimany and Kaisa Nyberg. Zero-Correlation Linear Cryptanalysis of Reduced-Round LBlock. *Des. Codes Cryptography*, Volume 73, issue 2, pages 683-698, May 2014.

II Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang and Yanfeng Wang. Reflection Cryptanalysis of PRINCE-like Ciphers. Accepted for publication in *J. Cryptology*, December 2013.

III Hadi Soleimany. Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro. Accepted for publication in *FSE 2014*, London, UK, March 2014.

IV Hadi Soleimany. Self-similarity Cryptanalysis of the Block Cipher ITUbee. Accepted for publication in *IET Information Security*, August 2014.

Author’s Contribution

Publication I: “Zero-Correlation Linear Cryptanalysis of Reduced-Round LBlock”

The current author is responsible for proposing the Matrix method to obtain zero-correlation characteristics, its application to LBlock, implementing the experiments and the related writing. The preliminary version of the paper under the same title was presented at International Workshop on Coding and Cryptography 2013. The extended version which also includes the application of the attack on TWINE is published in the special issue of the journal of Design, Codes and Cryptography.

Publication II: “Reflection Cryptanalysis of PRINCE-like Ciphers”

The current author is responsible for proposing the research topic and the main technique of applying the probabilistic reflection cryptanalysis on PRINCE. The preliminary version of the paper was submitted to International Workshop on Fast Software Encryption 2013 in collaboration with the members of the cryptography group at Aalto University. Since similar weaknesses had been identified by another group in parallel, the program committee members suggested to merge the two submitted papers. The final version of the paper was published at FSE 2013 and the full paper has been accepted for publication in the Journal of Cryptology.

Publication III: “Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro”

The current author is solely responsible for this work.

Publication IV: “Self-similarity Cryptanalysis of the Block Cipher ITUbee”

The current author is solely responsible for this work.

List of Acronyms

AES	Advanced Encryption Standard
DES	Data Encryption Standard
EMS	Even-Mansour Scheme
GE	Gate Equivalent
FFT	Fast Fourier Transform
ISO	International Organization for Standardization
ICT	Information and Communications Technology
IT	Information Technology
LLR	Log-likelihood ratio
LSB	Least-significant bit
MAC	Message Authentication Codes
MDS	Maximum Distance Separable
NAND	Negated AND or NOT AND
NIST	National Institute of Standards and Technology
p.d.	Probability distribution
RFID	Radio-Frequency Identification
S-box	Substitution-box
SPN	Substitution Permutation Network
XOR	bitwise exclusive OR

1. Introduction

The last decade has been marked by the rapid growth of small computing devices. Widespread deployment of constrained devices such as RFID tags changed from rarity to reality as they are becoming cheaper, smaller and more powerful. Decreasing size with manageable cost is one of the most significant changes in telecommunication and information technologies. Consequently, development in ICT is providing novel services that benefit from decreasing the size of computing devices. In this contest, the upcoming landscape of ICT involves not only combining a range of applications into one ubiquitous small device, but also a lot of constrained devices interacting with each other over a network, which is known as *"Internet of Things"*. The success of this process is dependent not only on the development of technologies, but also on the security of users and networks.

Due to the limitation of resources these pervasive devices are extremely limited in computing power, battery supply and memory which makes it hard to implement classical cryptographic primitives on them. These limitations leave us with the question of how to design a cipher suitable with respect to both efficiency and security. In other words, while this development opens tremendous opportunities for extensive new applications, it potentially poses a range of security risks which particularly demand for *lightweight ciphers* with novel structures to overcome the new threats.

In general, the significant challenges which have been encountered in designing lightweight ciphers can be attributed to three key parameters: security, cost, and performance. The main topic in designing modern lightweight ciphers is to develop inventive and unconventional structures to have a cipher with a small footprint, sufficient speed, reduced power consumption, while remaining sufficiently secure.

In response to the lack of suitable ciphers that are both efficient and secure for extremely constrained environments, several primitives have been proposed during the last years. With the growing prevalence of designing new lightweight primitives, it is important to analyze and quantify the cryptographic security of the novel structures that are emerging. Even though wide efforts over the past few years have been devoted to carry out a third party evaluation of the new designs, there is still an ongoing process of analyzing the security of novel structures.

In this dissertation, we choose lightweight block ciphers as our main topic and will try to construct innovative tools and methods to analyze the security of the recent designs with the hope to shed more light on this timely research subject.

1.1 Contributions of the Thesis

This dissertation consists of four publications that represent new contributions in the interrelated topics relevant to the field of cryptanalysis of lightweight block ciphers. This section gives an overview of the contributions of this work based on the published papers.

Publication I: Zero-correlation linear cryptanalysis is a novel extension of linear cryptanalysis. This paper shows how to adopt the Matrix method as an automatic tool to establish zero-correlation linear approximations. In particular, the method is used to obtain several zero-correlation linear approximations over 14 rounds of LBlock which lead to a key-recovery attack on a 22 reduced-round of the cipher. Most of the previous cryptanalyses of LBlock exploit the weakness in the key schedule of the initial version of the cipher and consequently, they are not applicable on the new version of LBlock that has a tweakable key schedule. The cryptanalysis presented in this work is independent of the key schedule and therefore also applies to the new version of LBlock. For the same reason and due to the structural similarities of the LBlock and TWINE block ciphers, the attack is also applicable on TWINE. Finally, the attack is implemented for a small variant of LBlock experimentally to validate the statistical model of zero-correlation linear cryptanalysis presented in [22].

Publication II: Reflection cryptanalysis as a particular form of self-similarity cryptanalysis is a well-known method against Feistel block ciphers. This work extends the application of reflection cryptanalysis to PRINCE-like ciphers which have an SPN structure by introducing a novel technique in the probabilistic setting. The core of PRINCE-like ciphers has a unique property called $\alpha-$reflection that is, the decryption function under the key K is equivalent to the encryption under the key $K \oplus \alpha$. This work studies the effect of the selection of the value α on security of the PRINCE-like ciphers. In particular, this work shows there exist some values of α that allow a key-recovery attack on the 10 rounds of PRINCE and 12 rounds of PRINCE$_{core}$. In addition, while the feasibility of related-key attack model in real-world applications is mostly treated with skepticism, this work shows how a strong related-key distinguisher can be exploited in the single-key model.

Publication III: Generalized Even-Mansour with a single key has been used in several lightweight block ciphers. This work describes a novel framework to enhance slide cryptanalysis against the general Even-Mansour scheme with one key in a probabilistic setting. The method exploits some features from related-key cryptanalysis, differential cryptanalysis and also probabilistic reflection cryptanalysis to build a particular differential characteristic which has potentially less active S-boxes than standard differential characteristics. In particular, the presented technique can overcome round-dependent constants which are the typical countermeasure against classical slide cryptanalysis. To demonstrate the effect of the presented method, we provide an analysis of two well-known lightweight block ciphers LED-64 and Zorro which lead to improve the best cryptanalysis presented by the designers of Zorro and the best results on 2-step reduced LED-64 in the known-plaintext model. The main result of this paper is to show that employing round constants is not always sufficient to provide security against a variant of slide cryptanalysis but the relation between the round constants should also be taken into account.

Publication IV: This work presents first third-party cryptanalysis of the lightweight block cipher ITUbee in the weak-key, related-key and single-key models. These results show that for a number of reasons, but mostly because of the relation between round constants, the probabilistic reflection distinguisher introduced in Publication II can be applied up to 10-round ITUbee for large classes of weak-keys. This is an interesting application, since ITUbee utilizes round-dependent constants with relatively high Hamming weight. This work demonstrates how the relation between round constants can be exploited in the conventional reflection cryptanalysis independent of their Hamming weight. This work further poses an interesting challenge to find an optimal way for choosing round-dependent constants.

1.2 Outline

This dissertation is based on articles and consists of a summary. The remainder of this summary is structured as follows:

Chapter 2 gives a short introduction into cryptographic primitives and their security goals. Chapter 3 gives an overview of block ciphers and presents the basic concepts used in this dissertation. In Chapter 4, we lay out the background considerations relevant to the theoretical foundation of linear cryptanalysis and its advanced extensions. Chapter 5 first covers the background material of the self-similarity cryptanalysis and provides a general introduction to the self-similarity cryptanalysis. Then novel probabilistic enhancements of these cryptanalyses are introduced. Chapter 6 summarizes the dissertation and suggests further research.

2. Cryptology

This chapter gives a general introduction to cryptographic concepts. We discuss the security goals of cryptosystems and define the models of cryptanalysis.

2.1 Cryptosystems

Cryptology is the art and science of securing communication between parties in order to keep information secret and unaltered by malicious parties. Modern cryptology can be divided into two general fields: *cryptography* and *cryptanalysis*. The aim of cryptography is to prevent leaking and tampering any information against any malicious attempts, called the *adversary*, by providing *cryptosystems*. On the other hand, the aim of cryptanalysis is to evaluate the security of cryptosystems.

There are several favorable properties which cryptosystems aim to provide. Among other things, primary objectives include:

Confidentiality: Information should be kept secret from all unauthorized parties and only the party who has the secret key should be able to obtain information.

Authentication: It should be possible for the receiver of a message to verify the origin of the received data.

Data integrity: It should be possible for the receiver to verify that the message has not been modified by an unauthorized party.

To achieve these goals, secure systems and networks employ fundamental cryptographic algorithms called *primitives*. These basic building blocks include, but are not limited to, encryption mechanisms, message authentication codes, and hash functions. Each primitive is applied for a particular purpose. The security and performance of the whole system highly relies on the employed primitives. As a result, primitives as building blocks should be reliably secure as well as efficient. Cryptographic primitives are not trusted until the security claim by the designers is evaluated rigorously by third-party experts.

2.2 Ciphers

A primitive which provides confidentiality between two parties (sender and receiver) over an untrusted channel is commonly called a *cipher*. Cipher is a public algorithm that makes use of secret information, called a *key*, to keep a message secure against an adversary. A cipher can be defined formally as follows:

Definition 1. *A cipher consists of the following elements:*

- $\mathcal{P}$ *is the message space and each* $p \in \mathcal{P}$ *is called plaintext.*
- $\mathcal{C}$ *is the cipher space and each element* $c \in \mathcal{C}$ *is called ciphertext.*
- $\mathcal{K}$ *and* $\mathcal{K}^*$ *are the key spaces of encryption and decryption, respectively.*
- $\mathcal{E}$ *is the set of encryption algorithms* $\{E_K : K \in \mathcal{K}\}$ *such that for each* $K \in \mathcal{K}$ *the encryption* E_K *is a one-to-one map from* $\mathcal{P}$ *to* $\mathcal{C}$.
- $\mathcal{D}$ *is the set of decryption algorithms* $\{D_{K^*} : K^* \in \mathcal{K}^*\}$ *such that for each* $K^* \in \mathcal{K}^*$ *the decryption* D_{K^*} *is a map from* $\mathcal{C}$ *to* $\mathcal{P}$. *In addition, for each* $K \in \mathcal{K}$ *there is a decryption key* $K^* \in \mathcal{K}^*$ *such that* $D_{K*}(E_K(p)) = p$ *, for all* $p \in \mathcal{P}$.

Sender and receiver must first confidentially agree on the keys in advance. The sender uses the encryption process to convert the plaintext to the ciphertext. The receiver uses corresponding decryption key and follows the decryption process to obtain plaintexts. If the encryption key is public for everybody then the cipher is called a *public-key* or asymmetric encryption mechanisms. Otherwise it is classified as a symmetric-key cipher in which decryption key is equal to the encryption key, or it can be obtained from the encryption key efficiently.

2.3 Security Goals

Kerckhoffs' principle states that the security of the cipher should rely only on the secret key [67]. This principle is widely appreciated by cryptographers, and was redefined by C. Shannon as "the enemy knows the system" in his seminal paper in 1949 [94]. Shannon took the first step in the direction of establishing the theory of secrecy systems by introducing two foundational concepts: *perfect security* and *computational security*.

2.3.1 Perfect Security

A cipher is perfectly secure if the ciphertext leaks no information, except its length, about the plaintext to someone without knowing the key. It can be interpreted in probability theory as $\Pr(P = p \mid C = c) = \Pr(P = p)$ for all $p \in \mathcal{P}$ and $c \in \mathcal{C}$. In other words the ambiguity of an adversary that has unlimited computational resources is not decreased by observing the ciphertexts. A well-known candidate cipher for achieving perfect security is the Vernam cipher, also called *one-time pad*, in which the plaintext is XORed simply by the key with the same length to produce the ciphertext [102]. Shannon proved that one-time pad achieves perfect security if the key is chosen uniformly at random and no two messages are encrypted using the same key.

2.3.2 Computational Security

In real-world applications, a cipher with perfect security is not practical since each message requires a new fresh key. In practice, the security of a cipher depends on the computational power of the attacker. This fact leads us to an alternative definition, which claims security against an adversary with limited computational capability. A cipher is said to be computationally n-bit secure if the most efficient attack to break the cipher requires at least 2^n operations. Typically the parameter n is equal to the length of the key (in bits), since a cipher can be broken by exhaustive search over all key candidates (see Section 2.4.3). Even under this definition, it is hard to prove computational security for a cipher, in general. There are two approaches in designing secure ciphers. The first approach is using *reduction* to show that breaking the cipher is at least as hard as solving a problem which is widely believed to be difficult. This approach is usually taken in public-key cryptography and is not necessarily a suitable choice for designing an efficient symmetric-key cipher. Shannon introduced another approach that has been a source of inspiration for designing ciphers. The leading idea is identifying twin properties of the operation for a secure cipher: *confusion* and *diffusion*. Confusion means the relation between the ciphertext and the key should be very complex. In particular, each bit of the ciphertext should depend on all bits of the key. Diffusion means each bit of the plaintext and the key should influence several digits of the ciphertext. Roughly speaking, each bit of the ciphertext should be changed with the probability $1/2$ if one flips one of the bits of the plaintext. Modern ciphers usually utilize permutations and S-boxes to provide diffusion and confusion, respectively. This common approach which is sometimes called *ad-hoc* approach, provides security against known cryptanalysis. One should keep in mind that ad-hoc proofs do not necessarily mean the cipher is provably secure, since it might be secure against one attack, but not against another attack.

2.4 Cryptanalysis

The objective of cryptanalysis is to obtain as much information as possible about hidden aspects of the cipher, i.e. the original data or the secret key. In this section, we classify cryptanalytic methods based on the type of information available to the adversary. Then we introduce complexity parameters to measure the resources required to mount an attack.

2.4.1 Cryptanalysis Scenarios

The attacker is assumed to have access to different types of information. In each attack, it should be precisely clarified what kind and how much of data is required to perform the attack. Data requirement can be an insurmountable bottleneck for an attack. We can outline a hierarchy of possible scenarios based on the type of data available to the attacker.

Ciphertext-only cryptanalysis: The attacker has access only to a certain number of ciphertexts.

Known-plaintext cryptanalysis: The attacker has access to a limited number of plaintexts and their corresponding ciphertexts.

Chosen-plaintext (ciphertext) cryptanalysis: The attacker can select a number of plaintexts (ciphertexts) and query the corresponding ciphertexts (plaintexts).

Adaptively chosen plaintext (ciphertext) cryptanalysis: The attacker can choose a number of plaintexts (ciphertexts) and ask the corresponding ciphertexts (plaintexts) while he has access to the previous plaintext-ciphertext pairs at each step before choosing the next query.

Related key: The attacker has access to a quantity of plaintext-ciphertext pairs under unknown keys that have a known relationship.

2.4.2 Cryptanalysis Complexity Parameters

The efficiency of an attack can be quantified by the following parameters that are used to measure the complexity of the attack.

Time complexity: Time complexity is the amount of computational operations required for mounting an attack. The computational unit is usually considered as the full encryption, since it is comparable to the exhaustive key search.

Data complexity: Data complexity is the expected amount of data required to perform the attack successfully.

Memory complexity: Memory complexity is the memory size required to perform the attack.

Success probability: The probability of success of the attack.

Since the required data should be obtained by performing the encryption function or the decryption function under the secret key, the complexity of an attack is usually defined as the dominant complexity among the above complexities. However, one should keep in mind that there exist several trade-offs between the different complexities (see Section 2.4.3).

2.4.3 Generic Cryptanalysis

There exist some cryptanalytic methods that are applicable to any cipher regardless of the internal specifications of the cipher. Such methods are referred as *generic cryptanalysis* in the sense that one cannot prevent the cipher against these attacks. The ultimate objective of the designers is to prevent the ciphers against cryptanalysis that can beat the boundaries given by generic cryptanalysis.

Exhaustive Key Search:

The most straightforward way to retrieve the secret key is to try try all possible values of the key exhaustively. For a cipher with a k-bit key, the probability of guessing the key correctly is 2^{-k}. As a result, regardless of the design of a cipher one can obtain the secret key in the worst case with

2^k encryptions and in the average time of 2^{k-1} encryptions.

Time-Memory Trade-off

M. Hellman was the first to exploit a general time-memory trade-off technique to break an arbitrary block cipher [47]. The technique can accelerate exhaustive search at the expense of requiring more memory allocated by an attacker. The technique can break a block cipher with N possible keys in time T with a trade-off relationship $TM^2 = N^2$ where M is allocated memory. In follow-up works, an improved trade-off of the form $TM^2D^2 = N^2$ between time T, memory M and data D is presented for stream ciphers where $D^2 \leq T \leq N$ [4, 17].

2.4.4 Outcome of Cryptanalysis

The main goal of cryptanalysis is to retrieve the secret key. However, it is not always possible, and the attacker might be able to recover some information about the key or the behavior of the cipher. L. Knudsen suggests a hierarchical classification of possible attacks as follows [74, 76]:

Total break: The attacker can find the secret key.

Global deduction: The attacker can find a function which is equivalent to the encryption or the decryption without finding the secret key.

Local deduction: The attacker can generate additional plaintexts (or ciphertexts) corresponding to previously unknown ciphertexts (or plaintexts).

Distinguishing attack: The attacker can efficiently distinguish the cipher from an ideal random permutation.

3. Block ciphers

In this chapter, we give an overview of block ciphers. The chapter starts with a short description of block ciphers. This is followed by a specification of the commonly used building block ciphers. After that, we discuss the criteria which are important for constrained applications such as area, power consumption, etc. Subsequently, we explain the choices that have been made in the process of designing lightweight block ciphers. Finally, we give a brief description of the lightweight block ciphers analyzed in this dissertation.

3.1 Introduction

A block cipher is a symmetric primitive which operates on a fixed length string of bits, called a *block*. A block cipher is a mapping which accepts two inputs: n-bit block P and k-bit key K where the parameters n and k are called *block size* and *key size*, respectively. The block cipher makes use of the secret key to transform the input block to another block of the same size. More formally, we can denote the encryption process of a block cipher as follows:

$E_K(P) := E(K, P) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$

Hence, the process of encryption can be seen as a set of 2^k different permutations. We note that for a set of 2^n n-bit blocks there exist $(2^n)!$ different permutations which are equal to $2^{(n-1.44)2^n}$, based on the Stirling's approximation. Thus, a block cipher with a practical key size can generate just a tiny fraction of all possible permutations. Roughly speaking, a secure block cipher is expected to build a permutation E_K randomly among all $2^{(n-1.44)2^n}$ possible permutations for a random key K.

3.2 Design Techniques

A broad class of block ciphers are designed by the repetition of an invertible transformation known as *round*. Each round maps a fixed-size block into a block with the same size by using a round key. The round keys which are referred to as *subkeys*, are derived from the initial secret key via an algorithm called *key schedule*. One advantage of iterated block ciphers with identical round functions is the existence of an efficient implementation, since one can make use of a similar code or hardware for each round. An extra advantage is giving more insights for establishing a secure design by exploiting well studied and relatively smaller parts. Using simple components with verified properties makes the analysis of the cipher much easier and clearer. Hence using the structures based on the iterated functions is a commonly adopted strategy for designing a "good cipher" which "should be hard to break and easy to implement" [78]. In the remainder of this section, we study typical structures used in the construction of block ciphers.

3.2.1 Feistel Ciphers

Feistel cipher is a well known iterative construction. Each round of an n-bit Feistel cipher consists of a round function followed by a swap operation except the last round which excludes the swap operation. In each iteration, the state is divided into two $n/2-$bit halves. The round function maps one half of the state to $n/2$ bits under the action of a k-bit subkey: $F : \{0,1\}^{n/2} \times \{0,1\}^k \rightarrow \{0,1\}^{n/2}$. After that, the half is XORed to the result one. Finally, the two halves of the state are swapped. The Feistel structure has the advantage of the round function not having to be invertible. In addition, the decryption for one key corresponds to the encryption with the round keys taken in the reverse order which allows the implementation of the decryption over the encryption with a negligible overhead. The most notable example of a Feistel based cipher is DES, which was selected as a national standard in 1976 by the US government.

3.2.2 Substitution-Permutation Network

Substitution-Permutation Network is another type of an iterated block cipher. As the name shows, each round of the cipher is constructed by the application of two basic components followed by key addition: a substitution and a permutation. The substitution layer is usually designed by combining a set of small nonlinear operations known as Substitution-boxes or S-boxes. S-boxes should be bijective to provide invertibility for the decryption process. Permutation is a linear layer that provides diffusion. Subkeys are combined to states by some group operations like addition or XOR.

3.2.3 Even-Mansour Scheme

In response to the vulnerability of DES against exhaustive search attacks, FX-construction was proposed by R. Rivest to establish an n-bit block cipher with $(2n+\kappa)$-bit key from a key-dependent function F with the κ-bit key. FX-construction consists of two n-bit pre- and post-whitening keys k_0 and k_2 which are XORed in the input and the output of the core function F which operated under the κ-bit k_1:

$FX_{k_0,k_1,k_2}(x) = k_2 \oplus F_{k_1}(k_0 \oplus x)$

J. Kilian and P. Rogaway proved this construction can achieve $(\kappa + n - 1 - \lg T)$-bit security for an ideal core function F where T is the number of pairs $(x, F_{K_1}(x))$ available to the attacker. This result shows that one can substantially increase the security of the cipher by a couple of simple operations, which can be an elegant approach for designers of lightweight block ciphers. S. Even and Y. Mansour took one step ahead in this direction. They considered a single public permutation as the simplest example of the core function and proved the lower bound for the time complexity of any attack on this scheme is $T = \Omega(2^n/D)$ where D is the number of known plaintexts available to the attacker. EM-scheme can be generalized directly by the iteration of more public permutations. Such a cipher construction can be seen as an instance of iterated block ciphers. A generalized EM-scheme is defined as $C = F_s(\cdots F_2(F_1(P \oplus K_1) \oplus K_2) \oplus K_3 \cdots \oplus K_s) \oplus K_{s+1}$ where we denote by K_i the key added to the state at the beginning of the i'th iteration and by K_{s+1} the last key. In the typical block ciphers each permutation, commonly known as *step*, is constructed with the iteration of simpler rounds.

3.2.4 ARX Structures

Several block ciphers use only a set of simple operations, modular addition, bit rotation, bit shift and XOR to provide the diffusion and confusion properties. These ciphers are usually referred to as ARX ciphers. ARX structures are a common alternative to the ciphers which are based on S-boxes. Due to the relatively fast and cheap implementation of these operations in software and hardware the ARX ciphers are more efficient than ciphers based on S-boxes. In addition, since their execution time is constant, they are immune against a *timing attack* in which the attacker analyzes the time taken to execute a cipher under different input values. As a down side, the rigorous security of a combination of these operations is typically not well understood. In particular, the properties of addition modulo n are under-researched, and their exact statistical behavior cannot estimated precisely in practice for large value of n [103]. In addition, since the diffusion of ARX structures is slow, the ARX ciphers require more rounds to achieve security against statistical cryptanalysis.

3.3 Lightweight Designs

Lightweight block ciphers are a rapidly growing field of symmetric cryptography that have extensive applications in diverse industries. Lack of secure lightweight ciphers has led to devastating attacks in extensively used applications like KeeLoq, which is used in remote keyless systems of cars. In response to this challenge, several lightweight block ciphers have been designed during the last years. In this section, we first introduce some early designs of lightweight block ciphers which have often later been found to be insecure. After that, we discuss the parameters which should be taken into account during the design process. Finally, we survey a number of popular properties of lightweight block cipher designs.

3.3.1 Obsolescent Lightweight Ciphers

The majority of both block ciphers and stream ciphers designed in the 1980s can be considered as lightweight ciphers due to the limitations of the available hardware platforms or the lack of suitable software at the time of design. Unsurprisingly, most of the obsolescent lightweight ciphers have been broken, since their design process has been proprietary without public evaluation. However, studying obsolescent lightweight ciphers is valuable, since they have shed more light on designing the new generation of lightweight ciphers. The list of insecure lightweight ciphers includes but is not limited to:

- Crypto1 is a stream cipher with 48-bit key algorithm designed by NXP Semiconductors for Mifare RFID tags. The cipher which has been widely used in smart cards is practically broken in the known plaintext model [39].

- Cryptomeria cipher (C2) is a 10-round Feistel block cipher which used to be employed for encrypting DVD Audio discs and Secure Digital cards [1]. C2 is broken with almost practical complexity and using adaptively chosen plaintexts [27].

- DECT is a stream cipher with a 64-bit key which was used widely in handsets and base stations in Germany. Nohl et al. presented an attack which can retrieve the secret key within hours [86].

- DST40 is a 200-round unbalanced Feistel block cipher with a 40-bit key which is developed by Texas Instruments and licensed by the 4C Entity. Due to the small size of the key, it is vulnerable to exhaustive search cryptanalysis.

- KeeLoq has been used widely in authentication systems of the car locks by various car manufacturers. An efficient combination of slide and meet-in-the middle techniques pose a practical attack on the cipher [52].

- Kindle is a stream cipher with 128-bit key which is used in the Amazon Kindle e-book reader. A. Biryukov et al. show that the cipher can be broken practically even in the ciphertext-only scenario [16].

3.3.2 Efficiency Parameters

The design goals of lightweight block ciphers encompass two major aspects which are equally important: security and efficiency. Block ciphers are designed with either suitable software or hardware implementation properties according to the intended applications. While hardware-optimized block ciphers can achieve high speed, software-optimized block ciphers benefit from flexibility and low cost. The performance of block ciphers can be assessed based on different metrics listed as follows [89]:

1. **Area:** Area of hardware implementation depends on the number of

logic gates required for the implementation of the cipher. A particular focus in designing a hardware-oriented lightweight block cipher is to make the hardware footprint as small as possible. To compare different block ciphers with respect to area requirement, one usually computes the technology-independent area based on a unit called *gate equivalent* (GE) which corresponds to a two-input NAND gate. In other words, the area is measured as the number of gate equivalents that is calculated by dividing the area of the implementation by the area of an NAND gate. Unlike its name, GE is not quite a standard measurement, since it still depends on what fabrication technology is used. Nevertheless expressing the area in terms of gate equivalent is common in the literature as a rough comparison between different implementations.

2. **Throughput:** Throughput of the cipher is the rate of a new ciphertext produced over time that is expressed in bits-per-second. Unlike standards ciphers, high throughput is usually not a goal design in lightweight block ciphers. However, moderate throughput is still required in most applications in constrained environments.

3. **Latency:** Latency is the delay time between an initial request of the encryption of a plaintext and producing a corresponding ciphertext. The latency is expressed by the clock cycles of the overhead. However, this does not necessarily mean all high-speed ciphers are low-latency [71]. Several important applications such as instant authentication protocols require a low-latency encryption with prompt response.

4. **Power Consumption:** To supply the required energy, constrained devices either rely on a strictly limited battery or they utilize an external electromagnetic field without an internal power source which makes low power consumption highly desirable. The gate level power is estimated by the Power Compiler based on switching activity. To have a fair comparison, one should keep in mind that power consumption strongly depends on clock frequency and what technology is used for the implementation.

However, there is always a trade-off among these parameters that makes it hard to compare different implementations. In addition, depending on the application, the implementation of the cipher can be optimized based on required properties. For example, if the applications require the encryption of just a small amounts of data, the implementations might be optimized for a small footprint whilst throughput is not equally important.

3.3.3 Security Goals

- **Moderate Security:** The typical applications of constrained devices are unlikely to require encryption of a large amount of data. This fact implies a notable limitation for the attacker in practice. On the other hand, the security level of the cipher should be chosen based on the value of the data. There is no point in investing more than required by the security level. For the relevant applications of the low-cost embedded devices, keeping the information secret forever is not required. Consequently, lightweight block ciphers have relatively small block and key sizes, since they aim to achieve a moderate rather than high level of security. 80-bit security is often adequate for moderate security and the block size usually varies between 32, 48 and 64 in the majority of lightweight block ciphers.

- **Side Channel:** In contrast to mathematical cryptanalysis, *Side channel cryptanalysis* exploits on information which is leaked from the implementation of the cryptographic algorithms rather than their mathematical weaknesses. An unprotected implementation against side-channel cryptanalysis can pose serious threats in practice, even if the cipher is theoretically secure. To mitigate side-channel cryptanalysis, a usual approach is to utilize additional elements like masking, to reduce the leakage of information from the implementation. Providing security against side-channel attacks by employing physical techniques certainly leads to extra cost in the implementation, which is challenging for low-resource applications. Thus the design of a block cipher and provision of its physical security have usually been done separately. Recently, some proposals considered security against side-channel cryptanalysis as an optimization criteria. In these block ciphers, possible side-channel measures are considered during the design process to keep protection costs as small as possible. Design goals of such lightweight block ciphers are twofold. On the one hand, the new structure should achieve moderate security with suitable performance. On the other hand, it should allow efficient protection of the cipher against side-channel cryptanalysis. The designers of Zorro, KLEIN and LS-family block ciphers followed this approach. In contrast to other block ciphers, LS block ciphers use look-up tables for the linear layer and implements S-boxes by logical operations. As another direction, Zorro in which consists of AES operations, uses only partial non-linear layers.

3.3.4 Popular Design Approaches

The designers of lightweight block ciphers have utilized a wide variety of methods to achieve the desirable goals introduced in Section 3.3.2. Each lightweight block cipher usually has an inventive structure as well as unconventional components. Nevertheless, we can still identify some typical properties exploited in a majority of lightweight block ciphers. In this section, we survey some ideas which have been used in recent designs.

- **Non-linear layer:** The nonlinear layer of block ciphers typically consists of a number of parallel S-boxes which are usually implemented as Boolean functions in the hardware. The designers usually choose all S-boxes identically since it allows a serialized implementation of the cipher which requires a significantly smaller area in comparison with the standard implementation. On the other hand, larger S-boxes can maximize nonlinearity and other good properties, but are more expensive as regards to hardware. Consequently, in pursuit of hardware efficiency and moderate security, major designs use 4-bit bijective S-boxes which are much more compact than usual 8-bit S-boxes in standard block ciphers like AES. However, software-oriented lightweight block ciphers like ITUbee can still utilize large S-boxes.

- **Key Schedule:** Block ciphers make use of a key schedule algorithm to expand the relatively short key into a number of subkeys. The key schedule utilizes a number of arithmetic operations to establish security against related-key and self-similarity cryptanalysis. However, a strong key schedule cannot be established for free. It has an impact on the latency, power consumption and size of the implementation. It is believed that the related-key cryptanalysis is very unlikely in the intended applications of lightweight block ciphers. In particular, the related-key setting is entirely alien for applications in which the key is *burnt* into the device. On the other hand, self-similarity cryptanalysis can be prevented by simple operations like round-dependent constants. In order to reduce the key set-up time and to have better performance, unconventional designs with mostly linear key-schedules, or even without key schedules, have been developed. In other words, the subkeys can be computed from the master key *on-the-fly* as they are almost identical. As a result, the computation of subkeys does not require any working memory. Simple key schedules have posed new challenges which we discuss later in Chapter 5.

- **Decryption over Encryption:** In some applications, *both* encryption and decryption should be implemented with low cost on the platform. In this context, one common approach is to make the decryption as similar as possible to the encryption to achieve a minimal overhead. By choosing involutory elements or constructions (like a Feistel structure), one can manage the implementation cost by sharing similarities between the encryption and decryption.

- **Linear Layer:** To have an efficient hardware-oriented lightweight block cipher, the linear layer of the block cipher should be chosen to maximize the diffusion while being implemented with minimum cost. MDS matrices are typically used in classical block ciphers as linear layers. Despite the great diffusion properties of MDS matrices, they are not suitable for constrained environments, since they are expensive to implement in hardware. Bit permutation is an efficient alternative with almost no cost and it has been widely used in lightweight block ciphers. We may also mention a promising method exploited in LED which makes the MDS matrix as a possible choice for the linear layer of lightweight block ciphers. J. Guo et al. introduced special MDS matrices that can be produced by iterating the multiplication of one light matrix denoted as *serial* [44, 45]. This trick is very hardware friendly although it might be slower in comparison with bit permutations.

3.4 Target Ciphers

In this section, we introduce prominent lightweight block ciphers which are analyzed in this dissertation.

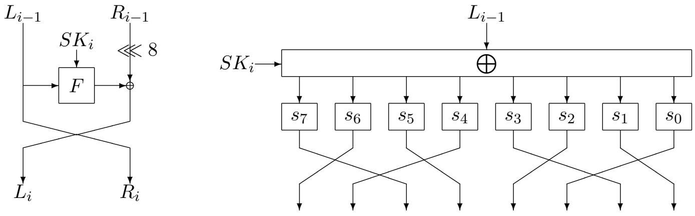

Figure 3.1. One round of LBlock and the round function

3.4.1 LBlock and TWINE

LBlock is a 32-round Feistel block cipher with 64-bit block length and supports a key length of 80 bits [109]. The function round of the cipher includes a key addition, eight different 4-bit to 4-bit S-boxes and a simple nibble-wise permutation as depicted in Figure 3.1. The key schedule of the original design had weaknesses that were exploited to mount the biclique cryptanalysis on the full-round LBlock. Subsequently, a new version of the cipher with a revised key schedule was presented by the designers [105]. The structure of LBlock encryption can be equivalently transformed into a decryption of an analogous cipher TWINE [100]. Nevertheless, there are two differences between TWINE and LBlock. TWINE uses identical S-boxes instead of eight different S-boxes and a different key schedule.

Publication I exploits the slow diffusion of the cipher to apply zero-correlation linear cryptanalysis on 22-round LBlock, which improves the previous results [63, 80, 92]. The key-recovery method described in this work does not exploit the properties of the key schedule neither S-boxes used in the cipher. Consequently, it is applicable to both variants of the LBlock as well as to TWINE. Recently Wu et al. exploit the relation between subkeys to extend the zero-correlation cryptanalysis presented in Publication I to 23-round of LBlock and TWINE [104].

3.4.2 Zorro

Zorro is a 128-bit block cipher and supports a key length of 128 bits [40]. The cipher can be seen as an instance of the generalized Even-Mansour scheme with one key. Zorro has 6 steps each of which consists of four rounds. The state can be conceptually illustrated as a 4×4 matrix where each cell represents a byte. Each round is composed of four operations in the following order:

1. SubCells applies the same 8-bit to 8-bit S-box on each of four bytes of the first row.

2. AddConstants adds round constants to the first row of the state. Let r be the number of the current round represented as a byte, for $1 \leq r \leq 24$. Then the round constant is defined as $(r \parallel r \parallel r \parallel r \ll 3)$.

3. ShiftRows cyclically shifts the i'th row by i byte(s) to the left.

4. MixColumns multiplies each column of the state by $M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$, over the field $GF(2^8)$ under the polynomial $x^8 + x^4 + x^3 + x + 1$.

Obviously, the round function of Zorro is the tweaked version of the AES round. While the last two operations are borrowed from AES, there are two differences between the nonlinear layers of AES and Zorro. The AES S-box is replaced by a new S-box, and it is applied on the partial state instead of the whole state. This innovative operation allows more efficient masking which is a popular countermeasure against side-channel cryptanalysis.

Publication III exploits the weaknesses in the structure and the rounds constants of Zorro to mount a probabilistic slide cryptanalysis on 16 rounds of the cipher. This improves the best cryptanalysis presented by the designers by four rounds. In addition, several weaknesses against differential and linear cryptanalysis have been revealed recently that allow to break the full-round cipher with the time complexity of 2^{45} by using about 2^{45} known plaintexts [6, 43, 90].

3.4.3 LED

LED is a 64-bit block cipher [45]. Two primary variants of the cipher are LED-64 and LED-128, which support the key sizes 64 and 128, respectively. The construction of LED-64 can be seen as an 8-step EMS with one key. Similarly, LED-128 is a 12-step EMS with two alternating keys. The 64-bit state is represented by a 4×4 matrix, where each cell represents a nibble. Similar to Zorro, each step includes four rounds of which consists of four AES-like transformations, but in different order:

1. AddConstants adds a round-dependent constant to the state.

2. SubCells applies a same 4-bit to 4-bit S-box in parallel on each of the 16 nibbles of the state.

3. ShiftRows cyclically rotates the i'th row by i nibble(s) to the left.

4. MixColumns multiplies each column by an MDS matrix $M = \begin{bmatrix} 4&1&2&2 \\ 8&6&5&6 \\ B&E&A&9 \\ 2&2&F&B \end{bmatrix}$, over the field $GF(2^4)$ under the polynomial $x^4 + x + 1$.

LED benefits from several hardware-friendly choices which implies one of the smallest footprint among lightweight block ciphers. In particular, the MDS matrix M used in the MixColumns operation can be seen equivalently as four applications of a hardware-friendly matrix A:

$$(A)^4 = \begin{bmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 4&1&2&2 \end{bmatrix}^4 = \begin{bmatrix} 4&1&2&2 \\ 8&6&5&6 \\ B&E&A&9 \\ 2&2&F&B \end{bmatrix} = M$$

LED aims to provide security against not only the classical cryptanalysis, but also against the related-key cryptanalysis. I. Dinur et al. present a generic cryptanalysis of the EM-construction that is applicable on the 3-step LED-64 and the 8-step LED-128 [36]. Meet-in-the-middle cryptanalysis have been applied up to the 2-step LED-64 [35, 54]. These results are improved for the 2-step reduced version of LED-64 by probabilistic slide cryptanalysis presented in Publication III which gives to the best cryptanalytic results on the 2-step reduced LED-64 in the known-plaintext model. In the related key model, F. Mendel et al. mount a key-recovery cryptanalysis on the 4-step LED-64 and the 8-step LED-128, respectively [82].

3.4.4 ITUbee

ITUbee is a 20-round Feistel block cipher that operates on 80-bit blocks and supports an 80-bit secret key [64]. To reduce memory requirement, ITUbee has almost no key schedule. The master key is divided into two equal parts $K = K_0||K_1$. In odd and even numbered rounds, the subkeys are alternatingly equal to K_1 and K_0. The keys $(K_0||K_1)$ and $(K_1||K_0)$ are used as pre- and post-whitening keys, respectively. ITUbee utilizes round-dependent constants to provide asymmetry in the subkeys as a countermeasure against self-similarity cryptanalysis. The round constants used

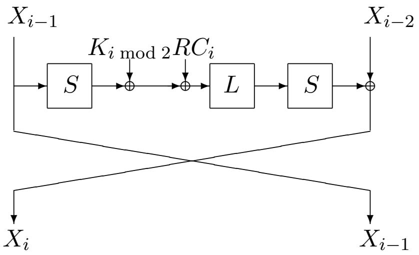

Figure 3.2. Round function of ITUbee

in the i'th round can be obtained simply as $(0x15 - i)||(0x29 - i)$.

The round function $F : \{0,1\}^{40} \rightarrow \{0,1\}^{40}$ is expressed as $F(X) = S(L(S(X)) \oplus RC_i \oplus K_{i \bmod 2})$ where the functions S and L are defined as follows:

- S is a nonlinear function which applies AES S-box on each of the bytes $X[i]$ for $0 \leq i \leq 4$.

- L is a linear byte-oriented function. If we represent the state X as a concatenation of five bytes $X = X[4]||X[3]||X[2]||X[1]||X[0]$, then the function L is expressed as the following equation: $L(X) = (X[4] \oplus X[3] \oplus X[0])||(X[4] \oplus X[3] \oplus X[2])||(X[3] \oplus X[2] \oplus X[1])||(X[2] \oplus X[1] \oplus X[0])||(X[4] \oplus X[1] \oplus X[0])$.

The best distinguisher presented by the designers covers at most 5 rounds of the cipher. Publication IV presents a first third-party cryptanalysis of ITUbee and mount a key-recovery cryptanalysis on 8 rounds of ITUbee. In addition, a reflection distinguisher on 10-round ITUbee is presented in Publication IV for a fraction of keys. These results significantly improve the best distinguisher presented in the original proposal by the designers.

3.4.5 PRINCE-like Cipher

The PRINCE-like ciphers is form a family of low-latency block ciphers. The PRINCE-like ciphers are based on the FX-construction described in Section 3.2.3. The $2n$-bit master key k is split into two equal parts $k = k_0||k_1$ and then extends to $3n$-bit $k_0||k_0'||k_1$ where k_0' is derived from k_0. The key k_1 is used as the key of a core function while the keys k_0 and k_0' are used as pre- and post-whitening keys, respectively. The core function, denoted by PRINCE$_{core}$, is an SPN cipher with $2R$ rounds. To reduce the

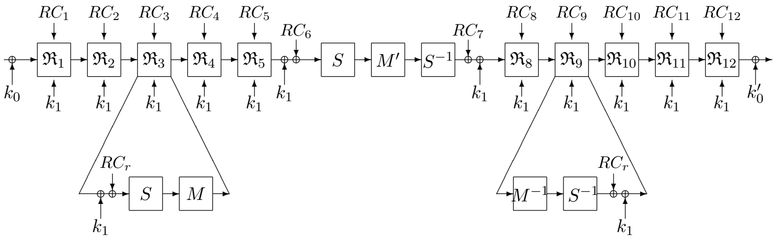

Figure 3.3. Description of a $(2R = 12)$-round PRINCE-like cipher

implementation cost of the decryption over the encryption, PRINCE$_{core}$ is designed with a property called α-reflection which means that the decryption of PRINCE$_{core}$ under the key k_1 is identical to the encryption with the key $k_1 \oplus \alpha$. The primary components of the core function are one non-linear layer S composed of a set of parallel S-boxes and two different linear layers defined by $n \times n$ matrices M' and M, where M' is an involutory matrix. Each of the first $R-1$ round functions $\mathfrak{R}_r$, for $1 \leq r \leq R-1$, consists of the addition of the round constant RC_r and the key k_1, the non-linear layer S and finally the linear permutation layer M. Each of the last $R-1$ rounds is defined in the reverse order $\mathfrak{R}_{R+1}, \cdots \mathfrak{R}_{2R}$. The two middle rounds $\mathfrak{R}_R$ and $\mathfrak{R}_{R+1}$ are defined differently. The summarized description of the rounds are given below:

$$\begin{array}{rcll}
\mathfrak{R}_r(x) &=& M\big(S(x \oplus RC_r \oplus k_1)\big) & \text{if } 1 \leq r \leq R-1 \\
\mathfrak{R}_r(x) &=& M'\big(S(x \oplus RC_r \oplus k_1)\big) & \text{if } r = R \\
\mathfrak{R}_r(x) &=& S^{-1}(x) \oplus RC_r \oplus k_1 & \text{if } r = R+1 \\
\mathfrak{R}_r(x) &=& S^{-1}\left(M^{-1}(x)\right) \oplus RC_r \oplus k_1 & \text{if } R+2 \leq r \leq 2R
\end{array}$$

The structure of PRINCE is depicted in Figure 3.3. To provide the α-reflection property for the PRINCE$_{core}$, the round constants are related palindromically by the parameter α such that the following holds:

$$RC_{2R-r+1} = RC_r \oplus \alpha, \text{ for all } r = 1, \ldots, 2R.$$

Due to the α-reflection property of the core function, PRINCE-like ciphers do not provide the same security level than the FX-construction. Given 2^m pairs of plaintext and corresponding ciphertext, this construction can achieve $(2n - m - 2)$-bit security [26, 55]. The original PRINCE is a sub-family of the PRINCE-like ciphers with $2R = 12$ rounds and $2n = 128$ bits of key. PRINCE has received a lot of attention by the cryptographic community. Various type of attacks on reduced versions of PRINCE have been published. J. Jean et al. described a key-recovery cryptanalysis against the 6-round PRINCE based on an integral distinguisher on the 4 middle rounds [55]. Publication II studies the effect of the choice of the value α by introducing a novel reflection distinguisher against PRINCE-like ciphers. In particular, this work shows that there exist some values of α that allow a key-recovery attack on the 10-round PRINCE and the 12-round PRINCE$_{core}$. Advanced meet-in-the-middle cryptanalysis against 8 and 9 rounds of PRINCE are presented in [30] and [79], respectively. These results are improved using multiple differential cryptanalysis which is applicable on up to 10 rounds of PRINCE [29].

4. Linear Cryptanalysis

Although the history of cryptanalysis dates back to ancient times, perhaps the most-revolutionary step in the history of modern cryptanalysis of symmetric primitives was the invention of differential [12] and linear cryptanalysis [81] that occurred during the analysis of DES. In this chapter, we intend to discuss linear cryptanalysis and its enhanced variants as indispensable cryptanalysis on block ciphers. This chapter starts with a short introduction to mathematical preliminaries. Then we give an overview of linear cryptanalysis. Subsequently, we introduce multidimensional linear cryptanalysis which exploits multiple linear approximations simultaneously in distinguishing or key-recovery cryptanalysis. Finally, we discuss zero-correlation linear cryptanalysis which is a novel extension of linear cryptanalysis.

4.1 Boolean Functions

We start by introducing some notation on Boolean functions. We denote the binary field by $\mathbb{F}_2$ and the linear space of n-dimensional vectors over $\mathbb{F}_2$ by $\mathbb{F}_2^n$. The canonical inner product of $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ where $a, b \in \mathbb{F}_2^n$, is defined as $a \cdot b = \sum_{i=1}^{n} a_i b_i$. In this notation the vector a is typically called the *linear mask* of b. A function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is called a *Boolean function*. We note that each linear Boolean function can be described as a mapping $x \mapsto a \cdot x$ for an appropriate a. Similarly, a function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ with $F = (f_1, \ldots, f_m)$, where the functions f_i for $1 \leq i \leq m$ are Boolean functions, is called a *vectorial Boolean function*. The *Hamming weight* $wt(a)$ of a vector $a \in \mathbb{F}_2^n$ is defined as the number of its nonzero coordinates, i.e. $wt(a) = |\{1 \leq i \leq n : a_i = 1\}|$. It is useful to study linear properties of Boolean functions in terms of a *Fourier coefficient* or a *Walsh transform*. The Fourier coefficient of a vectorial Boolean function

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ at the point $(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ is defined by

$$\hat{F}(a, b) = \sum_x (-1)^{b \cdot F(x) \oplus a \cdot x}.$$

4.2 Linear Approximation

Consider a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and let an input of the function be $x \in \mathbb{F}_2^n$. A *linear approximation* with an *input mask* $u \in \mathbb{F}_2^n$ and an *output mask* $v \in \mathbb{F}_2^m$ is defined as

$$x \mapsto u \cdot x \oplus v \cdot f(x).$$

The probability of this approximation can be computed as

$$p_f(u, v) = \Pr(u \cdot x \oplus v \cdot f(x) = 0)$$

and its *bias*, noted by $\epsilon_f(u, v)$, is defined as the distance of $p_f(u, v)$ from $1/2$, i.e.

$$\epsilon_f(u, v) = p_f(u, v) - \frac{1}{2}.$$

Due to scaling reasons, it is helpful to work with *correlation* defined as

$$c_f(u, v) = 2\epsilon_f(u, v).$$

In addition, it is usually more convenient to express the correlation of a linear approximation in terms of a Fourier coefficient. The relation between the Fourier coefficient of f and the correlation of a linear approximation can be derived as:

$$c_f(u, v) = \frac{\hat{f}(u, v)}{2^n}.$$

4.3 Linear Trail vs. Linear Hull

An encryption function can be seen as a vectorial Boolean function:

$$f : \mathbb{F}_2^n \times \mathbb{F}_2^k \to \mathbb{F}_2^n, f(x, K) = \mathcal{E}_K(x),$$

where $\mathcal{E}_K(x)$ is the encryption function of an n-bit block under a k-bit key. A linear approximation of a block cipher is defined as

$$u \cdot x \oplus v \cdot \mathcal{E}_K(x) = \omega \cdot K,$$

where $u, v \in \mathbb{F}_2^n$ and $\omega \in \mathbb{F}_2^k$. To apply linear cryptanalysis, one should find an approximation with a large absolute value of correlation $c(u, \omega; v)$.

Given an R-round iterated block cipher $\mathcal{E}_K(x) = f_R \circ \cdots \circ f_2 \circ f_1(x)$ where f_i is the i'th round function, a *linear trail* from u to v is a sequence of an intermediate mask linear in the form of $\theta = (\theta_0 = u, \theta_1, \cdots, \theta_{R-1}, \theta_R = v)$ where $\theta_i \in \mathbb{F}_2^n$ for $0 \leq i \leq R$. The correlation of one trail can be computed using the piling-up lemma with an assumption that all the intermediated linear approximations of rounds are independent:

$$p_\theta(u, v) = \frac{1}{2} + 2^{R-1} \prod_{i=1}^{R} (\epsilon_{f_i}(u_i, u_{i-1})),$$

as a result, the correlation of the linear trail is:

$$c_\theta = \prod_{i=1}^{R} c_{f_i}(u_i, u_{i+1}).$$

The correlation of a linear approximation (u, v) should be estimated by considering all linear trails with the input mask u and the output mask v, which is usually referred to as *linear hull* [87]. It is well known that the precise value of the correlation can be computed as the sum of the correlation of all R-round linear trails:

$$c_f(u, v) = \sum_{\theta | \theta_0 = u, \theta_R = v} c_\theta,$$

that is, the correlation of an approximation depends on the sign of correlations of the trails which in turn are determined by the round keys for common cipher structures. Linear cryptanalysis is applicable, if for almost all keys K, the correlation is large enough in absolute value. In general, it is hard to precisely estimate the distribution of the correlation over the key-dependent rounds. However, we can derive more information about a class of block ciphers, known as *key-alternating block ciphers*, in which the round function is applied in a particular form of $f_i(x, K_i) = F(x \oplus K_i)$. It is shown in [33, 87] that average squared correlation of an approximation in key-alternating block ciphers is the summation of the squared correlation of all trails.

Theorem 1 ([33, 87]). *For an R-round key-alternating block cipher $\mathcal{E}_K$ with the round function F, the following holds for any $u, v \in \mathbb{F}_2^n$ and $\omega \in$*

$\mathbb{F}_2^{Rn}$ *with the assumption of independent round keys* $K = (K_1, \ldots, K_R)$*:*

$$\begin{aligned} E_K[c(u \cdot x \oplus \omega \cdot K \oplus v \cdot \mathcal{E}_K(x))^2] &= E_K[c(u \cdot x \oplus v \cdot \mathcal{E}_K(x))^2] \\ &= \sum_{\theta|\theta_0=u,\theta_R=v} \prod_{i=0}^{R-1} c(\theta_i \cdot x \oplus \theta_{i+1} \cdot F(x))^2 \end{aligned} \tag{4.1}$$

Obviously, it is not feasible to consider all possible trails. In practice, the correlation is estimated by considering a limited number of trails from u to v which gives a lower bound of the squared correlation.

4.4 Key-recovery Cryptanalysis

The ultimate aim of most cryptanalysis is to recover the secret key of a cipher. In this section, we discuss the principles of recovering the key by mounting statistical cryptanalysis. In particular, we discuss two cryptanalytic techniques for applying linear cryptanalysis, which are known in the literature as Matsui's algorithms 1 and 2 [81].

4.4.1 Key-recovery Model

In a key-recovery cryptanalysis based on an efficient statistical distinguisher, an adversary attempts to determine the correct key among a set of key candidates by using a statistical measurement. It is assumed that the adversary can differentiate between the behavior of statistic T under the right key and other key candidates via observing a number of data, e.g., plaintext-ciphertext pairs. A general model of the key-recovery cryptanalysis consists of four phases [101]:

Counting Phase. The adversary invokes its oracle to collect the data required for distinguishing.

Analysis phase. For each key candidate, the adversary computes the statistic T based on the observed data.

Sorting Phase. The adversary sorts the key candidates in a list according to the computed value of T for each key.

Searching Phase. In the last step, the adversary exhaustively tries the key candidates from the top of the list until the right key is found.

All key-recovery cryptanalyses which exploit statistical distinguishers fall in this framework. One of the most-significant research areas has been finding the best statistic T, that is both easy to compute as well as efficient in differentiating the right key.

4.4.2 Matsui's algorithm 1

Given a linear trail $P \cdot u \oplus C \cdot v = k \cdot \omega$ with a correlation far from zero, Matsui's algorithm 1 describes a method of finding the parity bit of the subkey bits involved in the linear trail.

```
Matsui's algorithm 1
Input: $N$ known plaintext-ciphertexts pairs $(P, C)$.
Require: Counter $T$ for the number of times $P \cdot u \oplus C \cdot v = 0$.
  for all known plaintexts $(P, C)$ do
    if $P \cdot u \oplus C \cdot v = 0$ then
      Increment the counter T by one.
    end if
  end for
  if $T > N/2$ then
    guess $k \cdot \omega = 0$ (when $p > 1/2$) or $k \cdot \omega = 1$ (when $p < 1/2$).
  else
    guess $k \cdot \omega = 1$ (when $p > 1/2$) or $k \cdot \omega = 0$ (when $p < 1/2$).
  end if
```

The magnitude of the correlation determines the data complexity of the method, while it is assumed that the sign of the correlation depends on only the key bits involved in the linear trail. Debate is ongoing about the validity of this assumption, which has a crucial role in the success of the attack [34, 85]. In particular, the real correlation of a linear approximation might be estimated wrongly based on the linear hull effect [85]. A. Biryukov et al. extend Matsui's Algorithm 1 to obtain more information about the secret key [14]. M. Hermelin et al. exploit this method to show how it is possible to apply Matsui's Algorithm 1 without the assumption of statistical independence [51].

4.4.3 Matsui's algorithm 2

Let us consider a linear approximation with high correlation for the first $(r-1)$ rounds of an r-round block cipher $E_K(P) = \mathfrak{R}_r \circ \ldots \circ \mathfrak{R}_1(P)$. Matsui's algorithm 2 exploits a statistical test to recover some bits of the last round of the cipher. The primary idea is described as follows:

Matsui's algorithm 2

```
Input: $N$ known plaintext-ciphertexts pairs $(P,C)$, a linear approximation $(u,v)$ over $r-1$ rounds.
Require: Counters $T_{0,i}$ and $T_{1,i}$ for number of times $P \cdot u \oplus \mathfrak{R}^{-1}(C;k_i) \cdot v = 0$ and $P \cdot u \oplus \mathfrak{R}^{-1}(C;k_i) \cdot v = 1$, respectively where $k_i$ is a key candidate.
  for all all candidates $k_i$ do
    for all known plaintexts $(P,C)$ do
      Decrypt $C$ over the last round under $k_i$ and compute the binary value $b = P \cdot u \oplus \mathfrak{R}^{-1}(C;k_i) \cdot v$.
      Increment $T_{b,i}$ by one.
    end for
  end for
  Find the maximum value of $T_{b,i}$ and guess the last round key as the corresponding key candidate $k_i$.
```

The main idea of the method is based on an assumption that is known in the literature as *hypothesis of wrong-key randomization* [46]. Intuitively, the decryption of the ciphertext using a wrong key over the last round can be seen as one more encryption under a random key. Consequently, it is assumed that the plaintext P and $\mathfrak{R}_r^{-1}(C)$ under a wrong key are less dependent than the case when the correct key is used. This assumption also has a crucial impact on the accuracy of estimating the success probability and data complexity of the attack.

A considerable amount of literature has been dedicated to the accurate estimation of the success probability and data complexity of linear cryptanalysis. Matsui estimates the data complexity of the attack as the order of $|2\epsilon|^2$ for a certain success probability. In follow-up works, P. Junod et al. give detailed theoretical analysis for estimating the data complexity and success probability of this method [57, 58, 59]. Furthermore, Selçuk exploits a normal approximation for order statistics to present a thorough formula [93] based on the model described in [59].

Theorem 2 ([93], Theorem 2)**.** *Let P_S be the probability that a linear attack on an m-bit subkey, with a linear approximation of probability p, with N known plaintext blocks, delivers an a-bit or higher advantage. Assuming that the linear approximation's probability to hold is independent for each key tried and is equal to 1/2 for all wrong keys, we have, for a sufficiently* *large m and N,*

$$P_S = \Phi(2\sqrt{N}|p - 1/2| - \Phi^{-1}(1 - 2^{-a-1}))$$

Theorem 2 leads to a direct formula to estimate the amount of required known plaintexts for a certain success probability.

Corollary 3 ([93]). *With the assumptions of Theorem 2,*

$$N = (\Phi^{-1}(P_S) + \Phi^{-1}(1 - 2^{-a-1}))^2 \cdot |p - 1/2|$$

plaintext blocks are needed in a linear attack to accomplish an a-bit advantage with a success probability of P_S.

For more works related to the success rate and data complexity, we refer to [5, 20, 24].

4.5 Multidimensional Linear Cryptanalysis

Various extensions of linear cryptanalysis have been introduced which typically make use of multiple linear approximations with high correlation simultaneously [15, 56, 87]. A fundamental assumption of these approaches is statistical independence of linear approximations that is hard to verify for a general case in practice. In this section, we study multidimensional linear cryptanalysis introduced by M. Hermelin et al., which does not rely on the assumption that linear approximations are statistically independent [50]. We start by defining a fundamental term *capacity*, which is useful in computing the data required for multidimensional linear cryptanalysis.

4.5.1 Capacity

Let $p = (p_0, \ldots, p_M)$ and $q = (q_0, \ldots, q_M)$ be two discrete probability distribution of random variables with domain $\mathcal{D}$. The capacity between p and q is defined as follows:

Definition 2. *The Squared Euclidean Imbalance or capacity between two probability distribution p and q is defined by*

$$C(p, q) = \sum_{\eta \in \mathcal{D}} \frac{(p_\eta - q_\eta)^2}{q_\eta}.$$

In particular, the capacity between probability distribution p and the uniform distribution is denoted by $C(p)$ and called the capacity of p.

4.5.2 Multidimensional Linear Approximation

For a vectorial Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, let us consider m linear approximations $u_i \cdot x \oplus v_i \cdot f(x)$ where $1 \leq i \leq m$ such that linear masks (u_i, v_i) are linearly independent. Let us define functions $g_i(x)$ where $1 \leq i \leq m$ as

$$g_i(x) := u_i \cdot x \oplus v_i \cdot f(x).$$

We denote the correlation of g_i with C_i where $1 \leq i \leq m$ and refer to them as *base correlations*. Then the m-dimensional linear approximation of f is defined as

$$G(x) := Vf(x) \oplus Ux$$

where $V = (v_1, \ldots, v_m)$, $U = (u_1, \ldots, u_m)$ and $g = (g_1, \ldots, g_m)$. The probability distribution of the m-dimensional approximation denoted by $p = (p_0, \ldots, p_{2^m-1})$ can be computed in terms of the base correlations by using a method presented in [49].

Lemma 1. *For a vectorial Boolean function $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ with the probability distribution p and one-dimensional correlation C_a of $a \cdot g$ we have:*

$$p_\eta = 2^{-m} \sum_{a \in \mathbb{F}_2^m} (-1)^{\langle a, \eta \rangle} C_a$$

From Lemma 1, we have the following corollary which is derived by Parseval's relation [49].

Corollary 4. *For a vectorial Boolean function $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ defined as previously with the probability distribution p, we have:*

$$C(p) = \sum_{a \neq 0} C_a^2$$

4.5.3 Multidimensional Linear Distinguisher

Given a data set $\{x_1, \ldots, x_N\}$, empirical distribution q of the data sample is computed by

$$q_\eta = \frac{|\{1 \leq t \leq N : x_t = \eta\}|}{N}.$$

To decide whether the given data set is drawn from a cipher or not, we typically use two standard statistical approaches. One approach is useful for distinguishing an unknown probability distribution from a given set of probability distributions which is usually based on log-likelihood ratio

(LLR-statistic). Another approach is useful for deciding whether an empirical sample is drawn from a uniform distribution or not (goodness-of-fit method), which is usually based on the χ^2-statistic.

Likelihood Ration Distinguisher

In the LLR method, it is assumed that if the given data set is drawn from the cipher then the empirical distribution q belongs to one of the probability distributions $\{p^1, \ldots, p^n\}$, otherwise q looks uniform distribution θ. To decide if the given data is drawn from the cipher, an adversary computes the LLR-statistics for each key candidate:

$$LLR(q, p^i, \theta) = N \sum_{\eta \in \mathcal{D}} q_\eta \frac{p^i_\eta}{\theta_\eta}$$

If the maximum of LLR statistics is nonnegative, the adversary decides the data is drawn from the cipher. With the assumption that the probability distributions P_i where $1 \leq i \leq n$ are close to θ, the amount of data required for the LLR distinguisher is proportional to

$$N_{LLR} = \frac{\lambda}{\min_{1 \leq i \leq n} C(p_i)}$$

where λ is a constant that depends on the success probability [51].

χ^2 Distinguisher

In the χ^2 method, we wish to decide whether the given data set with an empirical distribution q is drawn from the random distribution or not. To decide this problem, an adversary computes the χ^2-statistic for each key candidate:

$$\chi^2(q; \theta) = N \sum_{\eta \in \mathcal{D}} \frac{(q_\eta - \theta_\eta)^2}{\theta_\eta},$$

where θ denotes the uniform distribution. A large value of $\chi^2(q; \theta)$ implies that the sample is not drawn from θ. We decide that the given data originates from the cipher (resp. random) if $\chi^2(q) \geq \tau$ (resp. $\chi^2(q) \geq \tau$), where τ is a threshold that depends on the error probabilities. The amount of data required for the χ^2 distinguisher is proportional to

$$N_{\chi^2} = \frac{\lambda\sqrt{M}}{C(p)}$$

where λ is a constant that depends on the success probability and $M = |\mathcal{D}|$ [48].

However, it is shown in [49] that the LLR method has a better performance. Consequently, the LLR method is used if the p.d. of linear approximations can be estimated accurately. Otherwise, the χ^2 method must be used.

4.6 Zero-correlation Linear Cryptanalysis

Zero-correlation linear cryptanalysis is a novel cryptanalytic technique proposed by A. Bogdanov and V. Rijmen [23] in 2012. In contrast to conventional linear cryptanalysis which takes advantage of linear approximations with high correlation, zero-correlation linear cryptanalysis is based on linear approximations with a correlation equal to zero for all keys. The bottleneck of the original proposal is the data complexity of cryptanalysis where almost the whole codebook is required. In a follow-up work, Bogdanov et al. proposed a novel framework to reduce the data requirement which exploits multiple independent linear approximations with a correlation of zero simultaneously [25]. To remove the independence assumption, a theoretical model was proposed based on the multidimensional linear distinguisher [22]. Publication I verified the validity of the model experimentally by implementing the distinguisher on a small variant of LBlock. The model presented in [22] has been applied widely to mount zero-correlation linear cryptanalysis on word-oriented block ciphers [19, 21, 99, 104, 106, 107, 108]. Publication I adopts the Matrix method to find zero-correlation approximations, which has been previously used in impossible differential cryptanalysis in [68, 69]. The connection between impossible differential distinguishers and zero-correlation distinguishers has been studied further by C. Blondeau et al. under particular circumstances for generalized Feistel ciphers [19]. As another direction, [21] introduced the application of the FFT technique with respect of speeding up the key-recovery phase of zero-correlation cryptanalysis for a class of block ciphers. The remainder of this section describes briefly how a multidimensional zero-correlation property can be used as a distinguisher for block ciphers.

4.6.1 Multidimensional Zero-correlation Cryptanalysis

Let us describe an arbitrary n-bit block cipher $E = E_f \circ E_c \circ E_b$ as the decomposition of the beginning rounds of E_b, center rounds of E_c and final rounds of E_f. Assume there exists m independent linear base approximations $u_i \cdot x \oplus v_i \cdot E_c(x)$ over the middle part of the cipher E_c where $1 \leq i \leq m$, and the masks $u_i, v_i \in \mathbb{F}_2^n$ are such that all $2^m - 1$ nonzero linear combinations of them have correlation zero. That is, for any non-zero m-bit string $\delta = (\delta_1, \dots, \delta_m)$ we have $c_{E_c}(\sum_{i=1}^m \delta_i u_i; \sum_{i=1}^m \delta_i v_i) = 0$. This distinguisher can be viewed as a multidimensional linear distinguisher with capacity zero. In multidimensional linear cryptanalysis the statistics is computed based on the probability distribution of the values of $z = (z_1, \dots, z_m)$. Given the correlations $c_{E_c}(\sum_{i=1}^m \delta_i u_i; \sum_{i=1}^m \delta_i v_i)$ the probability of the value z can be computed as follows

$$\begin{aligned}\Pr(z) &= \Pr(u_i x_i \oplus v_i y_i = z_i, \text{ for all } i = 1, 2, \dots, m) \\ &= 2^{-m} \sum_{\delta \in \mathbb{F}_2^m} (-1)^{\delta \cdot z} c_{E_c}(\sum_{i=1}^m \delta_i u_i; \sum_{i=1}^m \delta_i v_i).\end{aligned}$$

Hence the property that all the correlations $c_{E_c}(\sum_{i=1}^m \delta_i u_i; \sum_{i=1}^m \delta_i v_i)$ for non-zero δ vanish is equivalent to the property that the probability distribution of z is uniform.

With a similar technique to Matsui's Algorithm 2, the adversary observes a number N of distinct plaintext-ciphertext pairs under an unknown key. For each of the possible values of the subkeys, the adversary allocates a counter $V[z]$ for each of the value $z \in \mathbb{F}_2^m$ and initializes all $V[z]$ to zero. Then, for each distinct plaintext-ciphertext pair he partially encrypts the plaintext over the beginning rounds E_b and decrypts the corresponding ciphertext over the final rounds E_f up to the boundaries of the distinguisher. Then the adversary computes the value of the m-bit string $z = u_1 \cdot E_b(p) \oplus v_1 \cdot E_f^{-1}(c), \dots, u_m \cdot E_b(p) \oplus v_m \cdot E_f^{-1}(c)$ and increments the counter $V[z]$ by one. As it is shown in Publication I after this step, the adversary computes the value of the statistic T as follows:

$$T = \sum_{z=0}^{2^m-1} \frac{(V[z] - N2^{-m})^2}{N2^{-m}(1 - 2^{-m})}. \tag{4.2}$$

If $T < t$ where t is the decision threshold, the guessed key is put on a list $\mathcal{L}$. Finally, the correct key can be found from the exhaustive search manner over the list.

As shown in [36], the value T for the right key follows a χ^2 distribution with mean $\mu_0 = (2^m - 1)\frac{2^n - N}{2^n - 1}$ and variance $\sigma_0^2 = 2(2^m - 1)(\frac{2^n - N}{2^n - 1})^2$ while for a wrong key the distribution is a χ^2 distribution with mean $\mu_1 = 2^m - 1$ and variance $\sigma_1^2 = 2(2^m - 1)$. For the described distinguisher, we let α denote the probability that the cipher is discarded as a random permutation (type I error probability). In addition, we let β denote the probability that a random permutation is accepted as a cipher (type II error probability).

Given the error probabilities α and β with the decision threshold $t = \mu_0 + \sigma_0 z_{1-\alpha} = \mu_1 - \sigma_1 z_{1-\beta}$, the needed number of distinct known plaintexts is as follows:

$$N \approx \frac{(2^n - 1)(z_{1-\alpha} + z_{1-\beta})}{\sqrt{(\ell - 1)/2} + z_{1-\alpha}} + 1 \tag{4.3}$$

where $z_p = \Phi^{-1}(p)$, for $0 < p < 1$, and Φ is the cumulative function of the standard normal distribution [21].

4.6.2 Finding Zero-correlation Linear Approximations

Zero-correlation linear cryptanalysis can be viewed as a counterpart of *impossible differential cryptanalysis* which is a form of differential cryptanalysis based on a differential characteristic with probability zero [77]. The process of finding a linear approximation with correlation zero is similar to a specialized technique used for finding impossible differential characteristics, which is known in the literature as *miss-in-the-middle* [10]. The miss-in-the-middle technique proposes to detect an impossible differential characteristic by combination of two deterministic (truncated) differentials that lead to a contradiction in the middle. To detect a zero-correlation linear approximation, a similar technique is proposed to trace all linear approximation patterns of the input (resp. output) mask throughout the intermediate rounds in the encryption (resp. decryption) direction to obtain reachable approximations with nonzero correlation in the middle of a goal cipher. If the reachable approximations from the input mask and output mask do not match in an intermediate round then their combination is a zero-correlation approximation.

Publication I proposes to adopt the *Matrix method*, which originally was suggested to find impossible differential characteristic [68, 70], to automate the process of finding zero correlation linear approximation. In this section, we give a brief description of this cryptanalytic tool for finding zero-correlation linear approximation in word-oriented block ciphers with bijective functions.

Matrix Method

This method can be applied to a block cipher, where an n-bit state X is partitioned into m *words* of the same size n/m denoted by $X(i)$ where $1 \leq i \leq m$. To describe the propagation of a linear approximation over rounds, a linear mask is generally classified into the following five types:

1. zero mask, denoted by 0,

2. an arbitrary nonzero mask, denoted by $\overline{0}$,

3. nonzero mask with a fixed value a, denoted by a,

4. the exclusive-or of a fixed nonzero mask a and an arbitrary nonzero mask, denoted by $\overline{a}$,

5. any mask, denoted by $*$.

- If $Y(j)$ is not affected by a linear mask of $X(i)$ the value (i, j) is set to 0.

- If a linear mask of $X(i)$ affects $Y(j)$ directly the value (i, j) is set to 1.

- Finally if $Y(j)$ is affected by a linear mask of $X(i)$ over the round function F the value (i, j) is set to 1_F.

For the decryption of the round, another matrix is defined similarly. To construct the matrices we can use the following lemmas:

Lemma 2. ***XOR operation:*** *Let* $f(x_1, x_2) = x_1 \oplus x_2$. *Then the correlation of linear approximation* $u_1 \cdot x_1 + u_2 \cdot x_2 = v \cdot f(x_1, x_2)$ *is nonzero if and only if* $u_1 = u_2 = v$.

Lemma 3. ***Branching operation***[1]***:*** *Let* $f(x) = (x, x)$. *Then the correlation of linear approximation* $u \cdot x = (v_1, v_2) \cdot f(x)$ *is nonzero if and only if* $u = v_1 + v_2$.

Lemma 4. ***Bijective function:*** *Let* $f(x)$ *be a bijective function. If the correlation of a linear approximation* $u \cdot x = v \cdot f(x)$ *is nonzero then* $u = v = 0$*, or both* u *and* v *are nonzero.*

For a given state, we use the matrix iteratively to obtain the new state over multiple rounds by applying the arithmetic rules given in Table 4.1. To find a zero-correlation linear approximation, we compute the new states in both forward and backward directions until the values of all words become only $*$. Finally, we scan the intermediate values and check their incoherence.

[1] This Lemma is not presented in a correct way in Publication I.

Table 4.1. Arithmetic rules. The table of the left gives the addition rules between two mask types. The table on the right shows the operation rules of multiplication by 0, 1 and 1_F.

$+$	0	$\bar{0}$	a	$\bar{a}$	$*$
$\mathbf{0}$	$\mathbf{0}$	$\bar{0}$	a	$\bar{a}$	$*$
$\bar{0}$	$\bar{0}$	$*$	$\bar{a}$	$*$	$*$
b	b	$\bar{b}$	$a+b$	$*$	$*$
$\bar{b}$	$\bar{b}$	$*$	$*$	$*$	$*$
$*$	$*$	$*$	$*$	$*$	$*$

$\cdot$	0	1	1_F
0	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\bar{0}$	$\mathbf{0}$	$\bar{0}$	$\bar{0}$
a	$\mathbf{0}$	a	$\bar{0}$
$\bar{a}$	$\mathbf{0}$	$\bar{a}$	$*$
$*$	$\mathbf{0}$	$*$	$*$

Publication I utilizes the Matrix method to obtain several zero-correlation linear approximations over 14 rounds of LBlock which leads to a key-recovery attack on a 22 reduced-round of the cipher.

5. Self-similarity Cryptanalysis

A wide variety of cryptanalysis makes use of statistical properties of block ciphers. The complexity of such cryptanalysis relies on the non-random characteristics of a cipher which usually decrease as the number of rounds increases. In contrast, self-similarity cryptanalysis utilizes symmetric properties of the key schedule rather than the statistical properties of the block cipher. The effectiveness of the self-similarity cryptanalysis is usually not reduced by adding more rounds to the cipher. Despite the strength of the self-similarity techniques, their applications are limited to a small class of block ciphers, since they rely on a large degree of symmetric patterns in the key schedule like periodic subkeys. As a result, security against self-similarity cryptanalysis can be achieved with a well-designed key schedule that provides asymmetry in the subkeys. However, more complex key schedules tend towards higher cost and less performance such as high latency. Consequently, designers of lightweight ciphers usually utilize relatively straightforward approaches to break the similarity of the rounds. In particular, using round-dependent constants in lightweight block ciphers is a typical countermeasure against self-similarity cryptanalysis and one of the cheapest solutions for this purpose.

In this chapter, we focus on the limitations of the self-similarity cryptanalysis and make an effort to enhance its applications against lightweight block ciphers by pursuing novel, yet simple approaches. First, we describe *differential cryptanalysis* which will be used later in probabilistic self-similarity cryptanalysis. Then, we introduce *slide cryptanalysis* and *reflection cryptanalysis* as two significant examples of self-similarity techniques. After that, the state-of-the-art developments in this type of cryptanalysis are discussed. Finally, we describe related-key cryptanalysis in brief.

5.1 Differential Cryptanalysis

Differential cryptanalysis is a general cryptanalytic method based on finding a high correlation between a difference in the input and the resultant difference at the output of a block cipher [12]. Given an n-bit block cipher $\mathcal{E}_K(P) = f_R \circ \cdots \circ f_1(P)$, a *differential* is a pair $(\Delta_{in}, \Delta_{out})$ where $\Delta_{in}, \Delta_{out} \in \mathbb{F}_2^n$ and its probability is defined as

$$\Pr[\Delta_{in} \to \Delta_{out}] = \frac{|x \in \mathbb{F}_2^n | \mathcal{E}(P) \oplus \mathcal{E}(P \oplus \Delta_{in}) = \Delta_{out}|}{2^n}$$

In order to apply conventional differential cryptanalysis, one should find a differential with a high probability. The basic method of estimating the probability of a differential is to consider *differential characteristics*. A characteristic is constructed by concatenating a sequence of intermediate differentials $\Delta = (\Delta_0 = \Delta_{in}, \Delta_1, \ldots, \Delta_{R-1}, \Delta_R = \Delta_{out})$. Under the assumption of statistical independence between the differences in all rounds, the probability of the differential pair $(\Delta_{in}, \Delta_{out})$ can be computed as

$$\Pr[\Delta_{in} \to \Delta_{out}] = \sum_{\Delta} \prod_{i=1}^{R} \Pr[f_i(x) \oplus f_i(x \oplus \Delta_{i-1}) = \Delta_i]$$

In general, it is not feasible to precisely estimate the probability of differentials. A lower bound of the probability can be achieved by considering the probability of a few differential characteristics with dominant probabilities. When estimating the probability of a differential characteristic, the following properties are usually exploited:

1. The key addition in most ciphers is in the form of XOR. As a result, the difference between a pair of states (X, X') is not affected by the value of the key: $(X \oplus K) \oplus (X' \oplus K) = X \oplus X'$.

2. For a linear function F the relation $F(X) \oplus F(X') = F(X \oplus X')$ holds with a probability one.

3. Nonlinear layer of most block ciphers is constructed by small S-boxes. For this class of block ciphers, the probability of a differential characteristic depends only on S-boxes with nonzero input differences, since $S(x) \oplus S(x) = 0$ holds for an arbitrary S-box. We call these S-boxes *active* and other ones with zero input difference *passive*. The probability of

a one round differential characteristic is estimated by parallel applications of active S-boxes under the assumption that they are statistically independent.

In the remainder of this section, we briefly introduce a few extensions of differential cryptanalysis that are used in this chapter.

1. Related-key differential: It is observed by J. Kelsey et al. that in block ciphers with simple key schedules, the data difference can be controlled by the differences injected by the key difference in the related-key scenario [66]. In particular, if the key difference and the data difference are identical, they cancel each other, which leads to a smaller number of active S-boxes in the characteristic.

2. Impossible Differential: In contrast to conventional differential cryptanalysis, impossible differential cryptanalysis exploits differences with a probability of (exactly) zero [77].

3. Truncated Differential: Knudsen suggests an enhancement to differential cryptanalysis by considering a set of input and output differences [73]. Given an n-bit block cipher, we note a set of input and output differences by $\mathcal{D}_{in}$ and $\mathcal{D}_{out}$, respectively. The probability of the truncated differential is defined as follows:

$$\Pr[\mathcal{D}_{in} \to \mathcal{D}_{out}] = \frac{1}{|\mathcal{D}_{in}|} \sum_{\Delta_{in} \in \mathcal{D}_{in}} \sum_{\Delta_{out} \in \mathcal{D}_{out}} \Pr[\Delta_{in} \to \Delta_{out}]$$

A truncated differential with higher probability than the expected probability for uniform distribution, i.e. $\frac{|\mathcal{D}_{out}|}{2^n}$, can then be used to distinguish the cipher.

5.2 Slide Cryptanalysis

5.2.1 Conventional Slide Cryptanalysis

Consider an iterated block cipher which consists of identical round functions with a periodic key schedule. Depending on the key schedule, the cipher can be represented as an iteration of a single permutation F_k, where

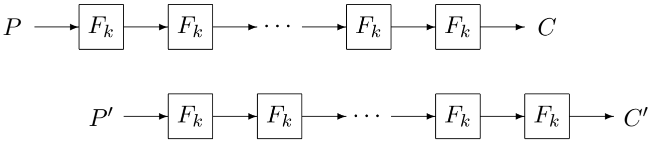

Figure 5.1. Slide cryptanalysis

F_k consists of one or more rounds of the cipher. The crucial observation is that, if plaintexts P and P' satisfy the relation $P' = F_k(P)$, due to the structure of the cipher, the relation $C' = F_k(C)$ holds for corresponding ciphertexts independently of the number of rounds as illustrated in Figure 5.1. Such a pair $((P, C), (P', C'))$ is called a *slid pair*. In general, $P' = F(P)$ occurs with probability 2^{-n} where n is the size of the block. Consequently, for an arbitrary n-bit block cipher, $2^{n/2}$ known plaintexts are required to expect one slid pair. Given enough slid pairs, the distinguisher can be converted to key-recovery cryptanalysis if F_k is susceptible to known-plaintext cryptanalysis. As a result, the total complexity of retrieving the secret key depends on three steps: preparing the required data, identification of slid pairs and retrieving the key using the slid pairs. The described attack has two major drawbacks compared to classical cryptanalysis. The first one is the difficulty of obtaining the key from the complex function F_K. In addition, its application has been restricted to a small class of ciphers due to the assumption of periodic subkeys.

5.2.2 Advanced Variants of Slide Cryptanalysis

In response to the major technical challenges in the application of slide cryptanalysis, a growing body of literature has been devoted to extending the primary method into generalized techniques that allow the application of the slide cryptanalysis to larger classes of block ciphers. In *complementary slide cryptanalysis*, one slides two instances of the encryption against each other to cancel the difference between the inputs of the rounds by a difference between the keys [18]. *Slide-with-a-twist* allows to slide an instance of the decryption against an instance of the encryption. *Realigning slide* is a technique in which two instances of the encryption are slid against each other while the middle of the cipher is unslid [88]. Furuya presented a technique aimed at providing several slid pairs simultaneously to carry out slide cryptanalysis on more complicated functions F_K [38]. Based on his crucial observation, if (P, P') is a slid pair, then $(F_K(P), F_K(P'))$ is also a slid pair. Biham et al. make use of the relation between cycle structure of the cipher to accelerate the identification process of slid pairs with the cost of using almost the whole codebook [11]. It is worth mentioning that slide cryptanalysis can be leveraged as a distinguisher on hash functions, nevertheless it is useless for finding collisions or (second) preimages [41, 91].

5.2.3 Probabilistic Slide Cryptanalysis

The conventional slide technique mentioned above relies on applying a deterministic relation between the corresponding ciphertexts of a slid pair. In contrast, Publication II pursues a probabilistic method of applying an enhanced slide cryptanalysis when the round functions are not entirely identical. This approach aims to infer the resultant difference $C \oplus F_s(C' \oplus K)$ based on the given difference $P' \oplus F_1(P \oplus K)$ with relatively high probability, what is not necessarily deterministic. In particular, we focus on a block cipher based on the general Even-Mansour scheme with one key which is widely used in designing lightweight block ciphers like Fantomas [42], LED, PRINTcipher [75], PRINCE, Robin and Zorro. In EMS with one key, protection against known slide attacks can already be achieved by introduction of round-dependent constants which are added to the data input at each round. The benefit of this method is obvious, that is, each round can be different without any additional cost. To circumvent the effect of different round constants, we exploit differential type characteristics in slide settings.

Let us consider a block cipher based on the general EMS with one key that consists of s different permutations $F_i(\cdot)$ for $1 \leq i \leq s$ as described in Section 3.2.3. Analogously to conventional slide cryptanalysis, we can slide one instance of the encryption against another instance of the encryption by one step. Due to the equality of subkeys, a differential type relation between the states can be obtained by tracing differences through the overall cipher, since the key has no influence on the difference between states. As a result, one can concatenate a sequence of appropriate differences $\mathcal{D} = \{\Delta_r : 0 \leq r \leq s-1\}$ such that $\Pr[F_r(x) \oplus F_{r-1}(x \oplus \Delta_{r-2}) = \Delta_{r-1}] = 2^{-p_{r-1}}$ where $0 \leq p_r$ and $2 \leq r \leq s$, to derive a differential type characteristic between the two encryption instances. This characteristic is illustrated in Figure 5.2. Under the assumption of statistical independence between the differences in all rounds, the probability of the characteristic can be estimated by $2^{-p} = \prod_{r=1}^{s-1} 2^{-p_r}$. Subsequently, $F_{s-1} \circ \cdots \circ F_1(x) \oplus F_s \circ \cdots \circ F_2(x \oplus \Delta_{in}) = \Delta_{out}$ holds with probability 2^{-p}

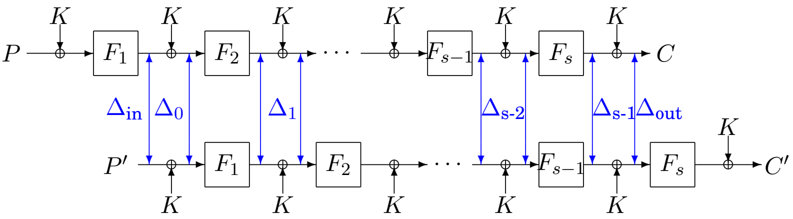

Figure 5.2. Slide cryptanalysis on general Even-Mansour scheme with one key

where $\Delta_{in} = \Delta_0$ and $\Delta_{out} = \Delta_{s-1}$. The characteristic can be exploited to differentiate the cipher from an ideal random oracle. Indeed, given $2^m = 2^{n/2+p/2}$ plaintexts and corresponding ciphertexts, there exist 2^{n+p} pairs of which 2^p are expected to satisfy the relation $F_1(P \oplus K) \oplus P' = \Delta_{in}$ for the unknown key. Analogously to the conventional slide, we expect to have one slid pair among these pairs, while for an ideal random permutation it occurs with probability 2^{p-n}.

Obviously, the amount of data required to mount an attack is deduced by utilizing a characteristic with a higher probability. In this direction, natural enhancement is to consider a set of L different output differences Δ^i_{out}, $i \in \{1, \cdots, L\}$ which directly lead to a decrease in data requirement. Nevertheless, this comes with the cost of repeating the key-recovery algorithm L times, thus allowing a trade-off between data and time complexities.

Probabilistic Slide Cryptanalysis of Zorro and LED-64

The described probabilistic framework is intriguing not only as a way to overcome the asymmetry in the subkeys but also as a way to exploit the relation between the round constants in order to provide more freedom in controlling the active S-boxes. In each round, a determined difference injected by the key difference potentially allows the cancellation of the data difference, which leads to a smaller number of active S-boxes in the characteristic. As an example, a four-round differential characteristic of LED-64 with 13 active S-boxes in slide setting is given in Publication II, while it is proven that the typical differential characteristic over four rounds of LED-64 has at least 25 S-boxes. This characteristic is then used for presenting the best results for the 2-step reduced LED-64 in the known-plaintext model. In addition, the existence of an efficient key-recovery method makes it feasible to efficiently convert the distinguisher to a key-recovery attack over one more step. As an illustration, a distinguisher over 12 rounds of Zorro is presented in Publication II which allows to mount a key-recovery attack on a 16-round version of cipher. This result improves the best cryptanalysis of this 24-round cipher presented by the designers, which could be applied up to 12.

5.3 Reflection Cryptanalysis

Reflection cryptanalysis is a form of self-similarity cryptanalysis introduced by O. Kara, which is based on the similarity between encryption and decryption functions [60]. As a result, involutory block ciphers with a palindromic key schedule are a natural target of reflection cryptanalysis. In particular, the application of reflection cryptanalysis against Feistel block ciphers has been widely studied. It benefits from the existence of notable fixed points in the middle of the target cipher [53, 61, 62]. The idea of utilizing fixed points in a Feistel structure is older and was already known during the studies on short cycles in repeated encryptions of DES under weak and semi-weak keys [31, 83]. However, Kara presents a framework for applying the same idea, not to weak keys, but instead, to the round functions of an involutory cipher under an unknown key. This section gives first a brief overview of reflection cryptanalysis. After that, we use novel techniques to extend the preliminary idea to the probabilistic setting, which leads to the first application of the reflection cryptanalysis on SPN block ciphers.

5.3.1 Basic Idea

Reflection cryptanalysis makes use of a non-uniform distribution of fixed points in the middle of an involutory block cipher. Under the assumption of the palindromically identical encryption and decryption round functions, intermediate fixed points can be extended to the next rounds using encryption and simultaneously reverted to the previous rounds using decryption as shown in Figure 5.3. This process can be described in detail as follows. Given an n-bit iterated block cipher with r rounds, we denote the round functions by R_{k_i} where $1 \leq i \leq r$ and k_i is the round key derived from the master key K. Using this notation, we can represent the $(j-i+1)$ intermediate rounds of the cipher starting from the i'th round as $R_K[i,j] = R_{k_j} \circ \cdots \circ R_{k_i}$ where $1 \leq i < j \leq r$. Let us denote the set of fixed points of the function $R_K[i,j]$ by $U_K[i,j] = \{x \in \mathbb{F}_2^n | R_K[i,j](x) = x\}$. The crucial observation is that if the relation $R^{-1}_{k_{i-t}} = R_{k_{j+t}}$ holds for $1 \leq t \leq u$, due to the palindromically identical encryption and decryption round

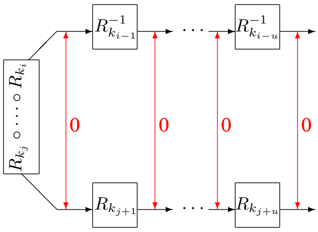

Figure 5.3. Reflection property under the assumption $R^{-1}_{k_{i-t}} = R_{k_{i+t}}$

functions, each intermediate fixed point $x \in U_K[i,j]$ can be propagated with the same property over $2u$ more rounds, that is $x \in U_K[i-u, j+u]$. In general, the effectiveness of reflection cryptanalysis directly depends on the probability of the existence of fixed points at the intermediate rounds, that is, $\Pr[x \in U_K[i-u, j+u]] = \frac{|U_K[i,j]|}{2^n}$. This property can be utilized to establish a distinguisher in a known-key model for an involution block cipher with notable fixed points in the middle of the cipher.

5.3.2 Reflection Distinguisher on Feistel Ciphers

An outline of a reflection distinguisher on an n-bit Feistel block cipher with r rounds is as follows: We let $P = (X_0||X_1)$ denote an n-bit plaintext. The encryption procedure can be described as a recursive function $X_{i+1} = f_{k_i}(X_i) \oplus X_{i-1}$ for $1 \leq i \leq r$ where $f : \mathbb{F}_2^{\frac{n}{2}} \rightarrow \mathbb{F}_2^{\frac{n}{2}}$ is the round function. Subsequently, the corresponding ciphertext is obtained as $C = (X_{r+1}||X_r)$. If $X_i = X_{i+1}$ holds, then the relation $X_{i-j} = X_{i+j+1}$ holds with probability one for $1 \leq j \leq u$, under the assumption $k_{i-t} = k_{i+t+1}$, for $0 \leq t \leq u-1$, where $1 \leq i \leq r-1$.

The main observation is that fixed points often naturally occur at the middle of the Feistel ciphers. Due to the structure of a Feistel with palindromically identical subkeys, the encryption functions after the fixed point will revert the state back to the plaintext. Therefore, the probability that $2u$-round of the cipher has a fixed point is $\Pr[X_{i-u}||X_{i-u-1} = X_{i+u+1}||X_{i+u}] = \frac{\#\{X_i = X_{i+1}\}}{2^n} = 2^{-n/2}$. For an ideal random permutation this probability is equal to 2^{-n}. Consequently, the $2u$-round cipher is distinguishable by using $2^{n/2}$ known plaintexts.

Publication IV exploits the relation between round constants to mount a reflection cryptanalysis up to 8 rounds of ITUbee. The most obvious finding of this work is that utilizing round-dependent constants with relatively high Hamming weight does not necessarily guarantee the security of the cipher against reflection cryptanalysis. While prior studies have noted the important role of round constants with low Hamming weights [37, 84, 98], Publication IV demonstrates how the relation between round constants can be exploited in a conventional reflection cryptanalysis independently of their Hamming weight.

5.3.3 Advanced Reflection Cryptanalysis

Let us now turn our attention to involution key-alternating block ciphers, in which the round function is of the form $R_i(x, K_i) = F(x \oplus K_i)$. Based on a conventional reflection property, intermediate fixed points $x \in U_K[i, i+j]$ can be extended over $2u$ more rounds if $K_{i-t} = K_{i+j+t}$ for $1 \leq t \leq u$. This condition implies a significant limitation on the key schedule which rarely hold for block ciphers. Building on previous works, Publication II generalizes the primary reflection idea to more general settings by introducing a non-deterministic framework based on non-uniformity properties of XOR difference between input data of round $i - t$ and corresponding output data of round $i + j + t$, for $1 \leq t \leq u$. In general, the framework can gain substantial improvements which enhance conventional reflection cryptanalysis for a larger number of rounds with the cost of increasing the number of required known plaintexts. We use X_r^I and X_r^O to denote the input and output states of the r'th round of an n-bit block cipher with R rounds, respectively. Suppose there exist a set of differences $\mathcal{D} = \{\delta_i \in \mathbb{F}_2^n : 0 \leq i \leq u\}$ such that the relation $X_{i-t} \oplus X_{i+t+1} = \delta_t$ holds for $0 \leq t \leq u$ with probability Pr_t where $u \leq i \leq R - u$. We call these relations as *reflection characteristics*. A reflection characteristic can be extended based on the following lemma in a probabilistic setting even if the subkeys are not palindromically equal.

Lemma 5. *Suppose the relation $X_{i-u} \oplus X_{i+u+1} = \delta_u$ holds. Then a relation $X_{i-u-1} \oplus X_{i+u+2} = \delta_{u+1}$ over two external rounds holds with probability*

$$\mathrm{Pr}_{u+1} = \mathrm{Pr}\left[F(X) \oplus F^{-1}(X \oplus \beta \oplus \delta_u) = \alpha\right]$$

where $\beta = K_{i-1} \oplus K_{j+1}$. □

For a cipher with an involution round function, the probability of a reflection characteristic can be computed by using techniques similar to the ones used in differential cryptanalysis, since functions F and its inverse F^{-1} are the same. For a reflection characteristic with a probability larger than 2^{-n}, the cipher is distinguishable from an ideal random permutation. The number of known plaintexts needed in the probabilistic reflection cryptanalysis is inversely proportional to the probability of the reflection distinguisher.

Publication IV demonstrates the application of this framework on ITUbee to extend conventional reflection cryptanalysis on 8 rounds of cipher over two more rounds for certain large classes of weak keys. The weakness properties we use are similar to those used in reflection cryptanalysis, however, now they are used in a probabilistic way. Publication II presents the first application of reflection cryptanalysis on an SPN block cipher. This work studies the effect of the value of α for PRINCE-like ciphers. For the weakest values of α, Publication II mounts key-recovery attacks on 10 and 12 rounds of PRINCE and PRINCE$_{core}$, respectively.

5.4 Related-key Cryptanalysis

The notion of *related-key* was first coined by E. Biham, who presented a general formalization of related-key cryptanalysis as a cryptanalytic model to assess the security of block ciphers [9]. The basic concept dates back to the 1980s, when the complementation property of DES was exploited to reduce the amount of searched key space by a factor of two. This notion was later expounded by M. Bellare and T. Kohno to more theoretical frameworks [7].

In general, the related-key cryptanalysis is a form of cryptanalysis where an attacker aims to derive some information about the key based on a disputable assumption that he is capable of obtaining the encryption of plaintexts or the decryption of ciphertexts under two or more unknown keys so that the relation between the keys is chosen by the attacker. Biham defined a relation over a pair of keys K and K^* so that all the subkeys derived from K can be obtained by shifting all the subkeys of K^* by one round backwards [9]. The same relation also was proposed independently by Knudsen for cryptanalysis of LOKI91, in which two keys have 14 common subkeys [72]. In essence, the relation between keys can be determined in a general rather than a particular type of relationship. Nevertheless, it is a common mindset that access to encryptions under related-key is very unlikely in most applications of block ciphers. This is the reason why related-key cryptanalysis usually is not of much practical interest, and has not been regarded as valuable as cryptanalysis based on the single-key oracles [8].

Despite these concerns, surprisingly some real-world cryptosystems have failed because of related-key cryptanalysis. Block ciphers often are used as building blocks of larger cryptosystems rather than standalone primitives. Consequently, related-key cryptanalysis may be practical in certain circumstances. This fact may also give more significance to related-key cryptanalysis. Consequently, most-modern block ciphers with broad applications are commonly expected to be accompanied by arguments in favor of sufficient security resistance to related-key techniques. In contrast, block ciphers with specific applications, like lightweight block ciphers, may ignore related-key attacks, since a related-key setting is disputable in their applications. In the remainder of this section, we study cases in which related-key distinguishers can threaten the security of block ciphers even as standalone primitives in the single-key model.

5.4.1 Related-key Cryptanalysis Towards Single-key Model

The existence of related-key characteristics can sometimes be exploited in order to mount a cryptanalysis in the single-key model. These cases are mostly confined to deterministic characteristics (see for example [65]). A deterministic relation between the encryption of DES under a key K and its complementation $\overline{K}$ was used to decrease the security of DES with one bit. We outline the basic principle of this original idea for a generalized case in which a deterministic related-key relation $E_K(P) \oplus E_{K\oplus\Delta}(P \oplus \Delta') = \Delta''$ holds for an arbitrary n-bit block cipher with an m-bit key where $\Delta', \Delta'' \in \mathbb{F}_2^n$ and $\Delta \in \mathbb{F}_2^m$. Without loss of generality, we assume the LSB of Δ is non-zero. We denote the set $\mathcal{K}$ as the subspace of all n-bit keys in which the LSB is zero: $\mathcal{K} = \{K \in \mathbb{F}_2^n, LSB(K) = 0\}$. The attack procedure is as follows:

1. Ask for the encryption of P and the encryption of $P^* = P \oplus \Delta'$ under an unknown key and save them as C and C^* respectively.

2. For all $K \in \mathcal{K}$

   - Compute $E_K(P)$; if it is equal to C, return K.

   - else, if $C \oplus \Delta'' = C^*$ return $K \oplus \Delta$.

The time complexity of the attack procedure is 2^{n-1} full encryptions of the cipher. The attack requires two plaintext-ciphertext pairs. The memory needed for the attack is negligible. Similarly, one can show that 2^m different deterministic related-key differential characteristics can be exploited to effectively reduce the key space to 2^{n-m} [13, 28].

Publication IV presents an application of the described technique on the 8-round reduced block cipher ITUbee using a novel deterministic related-key characteristic between the encryption and decryption functions. The property is derived by exploiting flaws in the key schedule and in the round constants that lead to the decrease of the security of 8-round ITUbee in the single-key model by one bit. As another application, Publication II implies that even non-deterministic related-key characteristics can be exploited in PRINCE$_{core}$ while this is not as straightforward as ITUbee. Due to the α-reflection property of PRINCE$_{core}$, the encryption function under the related-key $k_1 \oplus \alpha$ can be replaced by the decryption function under the original key k_1. This structure makes it possible to turn the related-key distinguisher to a cryptanalysis in the single-key model.

6. Conclusions

This last chapter provides a conclusive discussion of the main results accomplished in this dissertation, followed by an outlook on possible further research.

Related to the extension variants of linear cryptanalysis, we showed that the Matrix method can be used to facilitate the finding of a zero-correlation linear approximation. We utilized this tool to obtain several zero-correlation linear approximations for 14-round LBlock and TWINE. This leads to the retrieval of the secret key of the 22-round LBlock and TWINE regardless of their individual key schedules or S-boxes.

We also make use of the specification of inner components to enhance self-similarity cryptanalysis. In particular, the analyses in this dissertation give evidence that the relation between the round constants can be used to improve cryptanalytic results on lightweight block ciphers with simple key schedules. These results show that the exact security bounds against self-similarity cryptanalysis cannot be obtained without considering the relation between round constants.

Related to slide cryptanalysis, we presented a general framework in a probabilistic setting that allows the application of slide cryptanalysis on block ciphers with the Even-Mansour scheme with one key. After that, we show how to employ this framework in the analysis of recent design block ciphers Zorro and LED-64.

In the latter part of the thesis, we provided a new insight into reflection cryptanalysis by extending its application from Feistel block ciphers to the involutionary ciphers with SPN structure. As a result of the new cryptanalysis method presented in this dissertation, new design criteria concerning the selection of the value of α for PRINCE-like ciphers are obtained. In addition, we utilize this technique to reveal a certain structural weakness of ITUbee.

One natural direction for further research is to use the Matrix method or other techniques to find a better zero-correlation linear approximation, which would directly lead to more optimized key-recovery cryptanalysis.

In this dissertation, we take the first step towards the enhancement of self-similarity cryptanalysis in the probabilistic setting, which opens avenues for further research in cryptanalysis of block ciphers with simple key schedules. It remains to be studied whether the probabilistic slide cryptanalysis is applicable against other block ciphers. In particular, analyzing block ciphers based on the general Even-Mansour scheme like PRINCE, PRINTcipher and 3-WAY [32] as potential targets can be useful. Besides, the potential of probabilistic reflection cryptanalysis in the analysis of involution block ciphers with SPN structures is another interesting research direction.

The scenario of related-key methods has usually been considered as a strictly theoretical rather than a realistic attack model. The results presented in this dissertation show that the existence of strong related-key characteristics can sometimes be exploited in the single-key model. A natural question is how well the related-key distinguishers can lead to serious vulnerabilities in practice. In particular, it is an interesting question whether or not a huge amount of related-key characteristics with a relatively high probability can affect the security of a cipher in the single-key model.

Finally, the probabilistic approach presented in this dissertation for the enhancement of self-similarity cryptanalysis can serve as a basis for future studies in the analysis of authenticated encryption schemes which is a rapidly growing field of cryptography. Due to the lack of well-studied authenticated encryption schemes and the recent devastating attacks against worldwide applications like SSL [3], an international project CAESAR, funded by NIST, made a call for designs of new authenticated encryption schemes [2]. A total of 58 diverse proposals by cryptographers world-wide have been submitted by March 2014. The aim of the project is to create a portfolio of secure authenticated encryption schemes as a result of a public evaluation in four phases. One can make attempt to pursue the new perspective on slide cryptanalysis and reflection cryptanalysis obtained in this thesis by applying self-similarity cryptanalysis on some CAESAR proposal with simple round constants.

Bibliography

[1] C2 Block Cipher Specification, Revision 1.0 (2003), http://www.4Centity.com

[2] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, competitions.cr.yp.to/caesar.html

[3] AlFardan, N., Bernstein, D., Paterson, K., Poettering, B., Schuldt, J.: On the Security of RC4 in TLS. Royal Holloway University of London. Retrieved March 13, 2013.

[4] Babbage, S.: A Space/Time Tradeoff in Exhaustive Search Attacks on Stream Ciphers. European Convention on Security and Detection, IEE Conference Publication No. 408, May 1995.

[5] Baignères, T., Junod, P., Vaudenay, S.: How Far Can We Go Beyond Linear Cryptanalysis? In: Knudsen, L.R., Wu, H. (eds.) ASIACRYPT 2014. LNCS, vol. 7707, pp. 432–450. Springer (2004)

[6] Bar-On, A., Dinur, I., Dunkelman, O., Lallemand, V., Tsaban, B.: Improved Analysis of Zorro-Like Ciphers. Cryptology ePrint Archive, Report 2014/228 (2014), http://eprint.iacr.org/

[7] Bellare, M., Kohno, T.: A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer (2003)

[8] Bernstein, D.J.: Related-key Attacks: Who Cares? eSTREAM discussion forum (June 22, 2005), http://www.ecrypt.eu.org/stream/phorum/

[9] Biham, E.: New Types of Cryptanalytic Attacks Using Related Keys. J. Cryptology 7(4), 229–246 (1994)

[10] Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer (1999)

[11] Biham, E., Dunkelman, O., Keller, N.: Improved Slide Attacks. In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 153–166. Springer (2007)

[12] Biham, E., Shamir, A.: differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer (1990)

[13] Biham, E., Shamir, A.: Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 156–171. Springer (1991)

[14] Biryukov, A., Cannière, C.D., Quisquater, M.: On Multiple Linear Approximations. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 1–22. Springer (2004)

[15] Biryukov, A., Cannière, C.D., Quisquater, M.: On Multiple Linear Approximations. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 1–22. Springer (2004)

[16] Biryukov, A., Leurent, G., Roy, A.: Cryptanalysis of the "Kindle" Cipher. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 86–103. Springer (2012)

[17] Biryukov, A., Shamir, A.: Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 1–13. Springer (2000)

[18] Biryukov, A., Wagner, D.: Advanced Slide Attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 589–606. Springer (2000)

[19] Blondeau, C., Bogdanov, A., Wang, M.: On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) ACNS 2014. LNCS, vol. 8479, pp. 271–288. Springer (2014)

[20] Blondeau, C., Gérard, B., Tillich, J.P.: Accurate Estimates of the Data Complexity and Success Probability for Various Cryptanalyses. Des. Codes Cryptography 59(1), 3–34 (2011)

[21] Bogdanov, A., Geng, H., Wang, M., Wen, L., Collard, B.: Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In: Lange, T., Lauter, K., Lisonek, P. (eds.) SAC 2013. pp. 306–323. LNCS, Springer (2013)

[22] Bogdanov, A., Leander, G., Nyberg, K., Wang, M.: Integral and Multidimensional Linear Distinguishers with Correlation Zero. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 244–261. Springer (2012)

[23] Bogdanov, A., Rijmen, V.: Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Des. Codes Cryptography 70(3), 369–383 (2014)

[24] Bogdanov, A., Tischhauser, E.: On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 19–38. Springer (2013)

[25] Bogdanov, A., Wang, M.: Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 29–48. Springer (2012)

[26] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P.,

Thomsen, S.S., Yalçin, T.: PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications (Full version). Cryptology ePrint Archive, Report 2012/529 (2012), http://eprint.iacr.org/

[27] Borghoff, J., Knudsen, L.R., Leander, G., Matusiewicz, K.: Cryptanalysis of C2. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 250–266. Springer (2009)

[28] Brown, L., Kwan, M., Pieprzyk, J., Seberry, J.: Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 36–50. Springer (1991)

[29] Canteaut, A., Fuhr, T., Gilbert, H., Naya-Plasencia, M., Reinhard, J.R.: Multiple Differential Cryptanalysis of Round-Reduced PRINCE (Full version). In: FSE 2014. LNCS, Springer (to appear)

[30] Canteaut, A., Naya-Plasencia, M., Vayssière, B.: Sieve-in-the-Middle: Improved MITM Attacks. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013 (1). LNCS, vol. 8042, pp. 222–240. Springer (2013)

[31] Coppersmith, D.: The Real Reason for Rivest's Phenomenon. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 535–536. Springer (1986)

[32] Daemen, J., Govaerts, R., Vandewalle, J.: A New Approach to Block Cipher Design. In: Anderson, R.J. (ed.) FSE 1993. LNCS, vol. 809, pp. 18–32. Springer (1993)

[33] Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography, Springer (2002)

[34] Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography, Springer (2002)

[35] Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: Improved Linear Sieving Techniques withApplications to Step-Reduced LED-64. Cryptology ePrint Archive, Report 2012/712 (2012), http://eprint.iacr.org/

[36] Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES2. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013 (1). LNCS, vol. 8269, pp. 337–356. Springer (2013)

[37] Dinur, I., Dunkelman, O., Shamir, A.: Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized Internal Differentials. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 219–240. Springer (2013)

[38] Furuya, S.: Slide Attacks with a Known-Plaintext Cryptanalysis. In: Matsui, M. (ed.) ICISC 2002. LNCS, vol. 2288, pp. 214–225. Springer (2002)

[39] Gans, G.K., Hoepman, J.H., Garcia, F.D.: A Practical Attack on the MIFARE Classic. In: Grimaud, G., Standaert, F.X. (eds.) CARDIS 2008. LNCS, vol. 5189, pp. 267–282. Springer (2008)

[40] Gérard, B., Grosso, V., Naya-Plasencia, M., Standaert, F.X.: Block Ciphers That Are Easier to Mask: How Far Can We Go? In: Bertoni, G., Coron, J.S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 383–399. Springer (2013)

[41] Gorski, M., Lucks, S., Peyrin, T.: Slide Attacks on a Class of Hash Functions. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 143–160. Springer (2008)

[42] Grosso, V., Leurent, G., Standaert, F.X., Varici, K.: LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, Springer (to appear)

[43] Guo, J., Nikolic, I., Peyrin, T., Wang, L.: Cryptanalysis of Zorro. Cryptology ePrint Archive, Report 2013/713 (2013), `http://eprint.iacr.org/`

[44] Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer (2011)

[45] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer (2011)

[46] Harpes, C., Kramer, G.G., Massey, J.L.: A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-Up Lemma. In: Guillou, L.C., Quisquater, J.J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 24–38. Springer (1995)

[47] Hellman, M.E.: A cryptanalytic time-memory trade-off. IEEE Transactions on Information Theory 26(4), 401–406 (1980)

[48] Hermelin, M.: Multidimensional Linear Cryptanalysis. Ph.D. thesis, Aalto University School of Science and Technology (2010)

[49] Hermelin, M., Cho, J.Y., Nyberg, K.: Multidimensional Linear Cryptanalysis of Reduced Round Serpent. In: Mu, Y., Susilo, W., Seberry, J. (eds.) ACISP 2008. LNCS, vol. 5107, pp. 203–215. Springer (2008)

[50] Hermelin, M., Cho, J.Y., Nyberg, K.: Multidimensional Extension of Matsui's Algorithm 2. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 209–227. Springer (2009)

[51] Hermelin, M., Nyberg, K.: Dependent Linear Approximations: The Algorithm of Biryukov and Others Revisited. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 318–333. Springer (2010)

[52] Indesteege, S., Keller, N., Dunkelman, O., Biham, E., Preneel, B.: A Practical Attack on KeeLoq. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 1–18. Springer (2008)

[53] Isobe, T.: A Single-Key Attack on the Full GOST Block Cipher. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 290–305. Springer (2011)

[54] Isobe, T., Shibutani, K.: Security Analysis of the Lightweight Block Ciphers XTEA, LED and Piccolo. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 2012. LNCS, vol. 7372, pp. 71–86. Springer (2012)

[55] Jean, J., Nikolic, I., Peyrin, T., Wang, L., Wu, S.: Security Analysis of PRINCE. In: FSE 2013. LNCS, vol. 8424, pp. 92–111. Springer (2014)

[56] Jr., B.S.K., Robshaw, M.J.B.: Linear cryptanalysis using multiple approximations. In: Desmedt, Y. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 26–39. Springer (1994)

[57] Junod, P.: On the complexity of matsui's attack. In: Vaudenay, S., Youssef, A.M. (eds.) SAC 2001. LNCS, vol. 2259, pp. 199–211. Springer (2001)

[58] Junod, P.: On the optimality of linear, differential, and sequential distinguishers. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 17–32. Springer (2003)

[59] Junod, P., Vaudenay, S.: Optimal key ranking procedures in a statistical cryptanalysis. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 235–246. Springer (2003)

[60] Kara, O.: Reflection Cryptanalysis of Some Ciphers. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 294–307. Springer (2008)

[61] Kara, O.: Reflection Cryptanalysis of Some Ciphers. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 294–307. Springer (2008)

[62] Kara, O., Manap, C.: A New Class of Weak Keys for Blowfish. In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 167–180. Springer (2007)

[63] Karakoç, F., Demirci, H., Harmanci, A.E.: Impossible Differential Cryptanalysis of Reduced-Round LBlock. In: Askoxylakis, I.G., Pöhls, H.C., Posegga, J. (eds.) WISTP 2012. LNCS, vol. 7322, pp. 179–188. Springer (2012)

[64] Karakoç, F., Demirci, H., Harmanci, A.E.: ITUbee: A Software Oriented Lightweight Block Cipher. In: Avoine, G., Kara, O. (eds.) LightSec 2013. LNCS, vol. 8162, pp. 16–27. Springer (2013)

[65] Käsper, E., Rijmen, V., Bjørstad, T.E., Rechberger, C., Robshaw, M.J.B., Sekar, G.: Correlated keystreams in moustique. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 246–257. Springer (2008)

[66] Kelsey, J., Schneier, B., Wagner, D.: Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. In: Han, Y., Okamoto, T., Qing, S. (eds.) ICICS 1997. LNCS, vol. 1334, pp. 233–246. Springer (1997)

[67] Kerckhoffs, A.: La Cryptographie Militaire. Journal Des Sciences Militaires 9, 161–191 (1883)

[68] Kim, J., Hong, S., Lim, J.: Impossible differential cryptanalysis using matrix method. Discrete Mathematics 310(5), 988–1002 (2010)

[69] Kim, J., Hong, S., Sung, J., Lee, C., Lee, S.: Impossible Differential Cryptanalysis for Block Cipher Structures. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 82–96. Springer (2003)

[70] Kim, J., Kim, G., Lee, S., Lim, J., Song, J.H.: Related-Key Attacks on Reduced Rounds of SHACAL-2 3348, 175–190 (2004)

[71] Knezevic, M., Nikov, V., Rombouts, P.: Low-Latency Encryption - Is "Lightweight = Light + Wait"? In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 426–446. Springer (2012)

[72] Knudsen, L.R.: Cryptanalysis of LOKI91. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 196–208. Springer (1992)

[73] Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings. LNCS, vol. 1008, pp. 196–211. Springer (1994)

[74] Knudsen, L.R.: Contemporary Block Ciphers. In: Damgård, I. (ed.) Lectures on Data Security. LNCS, vol. 1561, pp. 105–126. Springer (1998)

[75] Knudsen, L.R., Leander, G., Poschmann, A., Robshaw, M.J.B.: PRINTcipher: A Block Cipher for IC-Printing. In: Mangard, S., Standaert, F.X. (eds.) CHES 2010. LNCS, vol. 6225, pp. 16–32. Springer (2010)

[76] Knudsen, L.R., Robshaw, M.: The Block Cipher Companion. Information Security and Cryptography, Springer (2011)

[77] Knudsen, L.R.: DEAL - A 128-bit Block Cipher. AES submission (1998)

[78] Lai, X.: On the Design and Security of Block Ciphers. ETH Series in Information Processing (1992), Hartung-Gorre Verlag Konstanz

[79] Li, L., Jia, K., Wang, X.: Improved Meet-in-the-Middle Attacks on AES-192 and PRINCE. Cryptology ePrint Archive, Report 2013/573 (2013), http://eprint.iacr.org/

[80] Liu, S., Gong, Z., Wang, L.: Improved Related-Key Differential Attacks on Reduced-Round LBlock. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 58–69. Springer (2012)

[81] Matsui, M.: Linear Cryptoanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer (1994)

[82] Mendel, F., Rijmen, V., Toz, D., Varici, K.: Differential Analysis of the LED Block Cipher. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 190–207. Springer (2012)

[83] Moore, J.H., Simmons, G.J.: Cycle Structures of the DES with Weak and Semi-Weak Keys. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 9–32. Springer (1987)

[84] Morawiecki, P., Pieprzyk, J., Srebrny, M.: Rotational Cryptanalysis of Round-Reduced Keccak. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 241–262. Springer (2013)

[85] Murphy, S.: The Effectiveness of the Linear Hull Effect. Report RHUL-MA-2009-19. Departmental Technical Report (2009).

[86] Nohl, K., Tews, E., Weinmann, R.P.: Cryptanalysis of the DECT Standard Cipher. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 1–18. Springer (2010)

[87] Nyberg, K.: Linear Approximation of Block Ciphers. In: Santis, A.D. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 439–444. Springer (1995)

[88] Phan, R.C.W.: Advanced Slide Attacks Revisited: Realigning Slide on DES. In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS, vol. 3715, pp. 263–276. Springer (2005)

[89] Poschmann, A.Y.: Lightweight cryptography: cryptographic engineering for a pervasive world. Ph.D. thesis (2009), published: Ph.D. Thesis, Ruhr University Bochum

[90] Rasoolzadeh, S., Ahmadian, Z., Salmasizadeh, M., Aref, M.R.: Total Break of Zorro using Linear and Differential Attacks. Cryptology ePrint Archive, Report 2014/220 (2014), `http://eprint.iacr.org/`

[91] Saarinen, M.J.O.: Cryptanalysis of Block Ciphers Based on SHA-1 and MD5. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 36–44. Springer (2003)

[92] Sasaki, Y., Wang, L.: Comprehensive Study of Integral Analysis on 22-Round LBlock. In: Kwon, T., Lee, M.K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 156–169. Springer (2012)

[93] Selçuk, A.A.: On probability of success in linear and differential cryptanalysis. J. Cryptology 21(1), 131–147 (2008)

[94] Shannon, C.: Communication Theory of Secrecy Systems. Bell System Technical Journal 28, 656–715 (1949)

[95] Soleimany, H.: Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, Springer (to appear)

[96] Soleimany, H.: Self-similarity Cryptanalysis of the Block Cipher ITUbee. IET Information Security (to appear)

[97] Soleimany, H., Blondeau, C., Yu, X., Wu, W., Nyberg, K., Zhang, H., Zhang, L., Wang, Y.: Reflection Cryptanalysis of PRINCE-like Ciphers. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 71–91. Springer (2014)

[98] Soleimany, H., Blondeau, C., Yu, X., Wu, W., Nyberg, K., Zhang, H., Zhang, L., Wang, Y.: Reflection Cryptanalysis of PRINCE-like Ciphers. Journal of Cryptology (to appear)

[99] Soleimany, H., Nyberg, K.: Zero-correlation linear cryptanalysis of reduced-round LBlock. Des. Codes Cryptography 73(2), 683–698 (2014)

[100] Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE : A Lightweight Block Cipher for Multiple Platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 339–354. Springer (2012)

[101] Vaudenay, S.: An Experiment on DES Statistical Cryptanalysis. In: Gong, L., Stearn, J. (eds.) ACM Conference on Computer and Communications Security. pp. 139–147. ACM (1996)

[102] Vernam, G.: Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. Journal of the IEEE 55, 109–115 (1926)

[103] Wallén, J.: Linear approximations of addition modulo 2^n. In: Johansson, T. (ed.) FSE. LNCS, vol. 2887, pp. 261–273. Springer (2003)

[104] Wang, Y., Wu, W.: Improved Multidimensional Zero-Correlation Linear Cryptanalysis and Applications to LBlock and TWINE. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 1–16. Springer (2014)

[105] Wang, Y., Wu, W., Yu, X., Zhang, L.: Security on LBlock against Biclique Cryptanalysis. In: Lopez, J., Tsudik, G. (eds.) WISA 2012. LNCS, vol. 7690, pp. 1–14. Springer (2012)

[106] Wen, L., Wang, M.: Integral Zero-Correlation Distinguisher for ARX Block Cipher, with Application to SHACAL-2. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 454–461. Springer (2014)

[107] Wen, L., Wang, M., Bogdanov, A.: Multidimensional Zero-Correlation Linear Cryptanalysis of E2. In: Pointcheval, D., Vergnaud, D. (eds.) AFRICACRYPT 2014. LNCS, vol. 8469, pp. 147–164. Springer (2014)

[108] Wen, L., Wang, M., Bogdanov, A., Chen, H.: Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard. Inf. Process. Lett. 114(6), 322–330 (2014)

[109] Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344. Springer (2011)

DISSERTATIONS IN INFORMATION AND COMPUTER SCIENCE

Aalto-DD138/2014	Sovilj, Dušan Learning Methods for Variable Selection and Time Series Prediction. 2014.
Aalto-DD144/2014	Eirola, Emil Machine learning methods for incomplete data and variable selection. 2014.
Aalto-DD149/2014	Äijö, Tarmo Computational Methods for Analysis of Dynamic Transcriptome and Its Regulation Through Chromatin Remodeling and Intracellular Signaling. 2014.
Aalto-DD156/2014	Sjöberg, Mats From pixels to semantics: visual concept detection and its applications. 2014.
Aalto-DD157/2014	Adhikari, Prem Raj Probabilistic Modelling of Multiresolution Biological Data. 2014.
Aalto-DD171/2014	Suvitaival, Tommi Bayesian Multi-Way Models for Data Translation in Computational Biology. 2014.
Aalto-DD177/2014	Laitinen, Tero Extending SAT Solver with Parity Reasoning. 2014.
Aalto-DD178/2014	Gonçalves, Nicolau Advances in Analysis and Exploration in Medical Imaging. 2014.
Aalto-DD191/2014	Kindermann, Roland SMT-based Verification of Timed Systems and Software. 2014.
Aalto-DD207/2014	Chen, Xi Real-time Action Recognition for RGB-D and Motion Capture Data. 2014.

Aalto-DD 211/2014

9 789526 060255

ISBN 978-952-60-6025-5 (printed)
ISBN 978-952-60-6026-2 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

Aalto University
School of Science
Department of Information and Computer Science
www.aalto.fi