Doctoral Thesis

Design and Analysis of Diffusion in Feistel-Type Symmetric-Key Cryptosystems

January 2022

Graduate School of Engineering, Nagoya University

Kyoji Shibutani

Acknowledgement

I would like to express my gratitude to all those who supported me during the course of my Ph.D study. First and foremost, I would like to express my sincere gratitude to my supervisor Associate Professor Tetsu Iwata for giving me the opportunity to study at Nagoya University. Without his patience, encouragement and expert guidance, this thesis could not have been completed. I would also like to thank the jury members of this thesis, Professor Nobuo Kawaguchi, Professor Shao-Liang Zhang, Professor Shoichi Hirose (University of Fukui) and Professor Noboru Kunihiro (University of Tsukuba) for reviewing the drafts and giving me valuable feedbacks.

I would like to thank Taizo Shirai who guided me as a mentor when I started my career as a researcher in the company. He taught me many things from the basic things on cryptography to the fun of the research. I would also like to thank Takanori Isobe for invaluable discussions on cryptography. His great inspirations always stimulated me a lot. I would like to thank all (ex)-colleagues in the same division, especially to Toru Akishita, Asami Mizuno and Yasuaki Honda for their continuous support.

I would like to thank Professor Bart Preneel for giving me the opportunity to study at COSIC in Katholieke Universiteit Leuven. With many great cryptographers, I spent great time as a researcher there. I could have several results related to this thesis during and after studying at COSIC. I would like to thank many COSICs, especially to Vesselin Velichkov, Nicky Mouha, Christian Rechberger, Sebastiaan Indesteege, Özgül Küçük, Kerem Varici, Denis Toz and Elmar Tischhauser, who studied in the same room and the room next door at that time. I greatly appreciate my coauthor Andrey Bogdanov for insightful discussions. Without his expert advice and comments, I could not further improve my results.

My last appreciation is for my family. I express my thankfulness to my parents, my son and my daughter for their intentional or unintentional encouragement. Finally, I deeply appreciate my wife, Ayumi, for her understanding, kind support, quiet patience and continuous encouragement during my Ph.D study, without which this thesis would never have been possible.

Kyoji Shibutani
January 2022

Abstract

Information security is a crucial technology for people all over the world to live safely and securely. It consists of several technologies including network security and application security to mainly ensure confidentiality, integrity and availability. Among them, cryptography is a fundamental technology to design information security applications. Cryptography provides several important functionalities including authenticity, confidentiality, integrity and randomness. It also has several categories and two fundamental technologies are known as public-key and symmetric-key cryptography. We focus on the latter one including block ciphers, cryptographic hash functions and stream ciphers. The main advantage of symmetric-key cryptography compared to public-key cryptography is its high computational performance. Thus, symmetric-key cryptography is necessary for most information security applications even when public-key cryptography is used in the applications.

A block cipher, one of symmetric-key primitives, is a keyed permutation used for encrypting and decrypting digital data by a given secret key. It has much wider applications than just data encryption. In fact, it has been well known as modes of operation that it provides several functionalities including authenticity and data integrity by using a block cipher as a component. Namely, if we have a good block cipher, we can easily derive several cryptographic applications such as a cryptographic hash function, a stream cipher and a message authentication code by using the block cipher as a component. Therefore, a block cipher is considered to play a central role in symmetric-key primitives.

A modern block cipher typically has iterative structure which iteratively utilizes a round function consisting of nonlinear functions and linear functions. The confusion and diffusion, which are known as two important properties for designing a secure block cipher, are considered to be provided by nonlinear functions and linear functions, respectively. The research related to the confusion including a method to design a good small nonlinear permutation called S-box has been well studied. On the other hand, there still exist some rooms to improve the diffusion. In general, a cipher with slow diffusion requires a lot of iterations to be secure, and then takes a long encryption / decryption time. Therefore, improving the diffusion is crucial for designing an efficient and secure block cipher.

While various structures have been proposed to design a block cipher, Substitution Permutation Networks (SPNs) and Feistel-type structures have been known as two main structures among them. SPNs consist of a substitution layer (several small nonlinear maps referred to as S-boxes applied in parallel) and a permutation layer (also known as a linear diffusion layer) in a round. One of the advantages of SPNs compared to Feistel-type structures is its fast diffusion, since all input data are converted by a substitution layer and a permutation layer in a round. On the other hand, SPNs require an inverse function for a decryption. This implies that an encryption function and a decryption

function are required to be separately implemented for SPNs. Feistel-type structures divide input data into more than two sub-blocks, then almost half of them are converted by nonlinear functions called F-functions in a round. In other words, almost half of the input data are unchanged in a round. In contrast to SPNs, the main advantage of Feistel-type structures is the involution property which does not require an inverse function for a decryption. That is, for Feistel-type structures, only an encryption function is required to be implemented for both encryption and decryption. Moreover, the size of F-functions, nonlinear functions used in Feistel-type structures, in a round is almost half compared to that of SPNs. These properties lead to a compact implementation. On the other hand, its main drawback is slow diffusion compared to SPNs, since almost half of the input data are unchanged in a round.

This thesis is dedicated to design and analysis of diffusion in Feistel-type symmetric-key cryptosystems including balanced Feistel networks (BFNs) and generalized Feistel networks (GFNs). BFNs and d-line GFNs divide input data into two and d sub-blocks, respectively, where $d > 2$ is a positive integer. Thanks to the involution property which does not require an inverse function for a decryption, Feistel-type constructions are known to be implemented more compact than SPNs. However, it has been well known that the diffusion of Feistel-type constructions is slower than that of SPN-type constructions. Despite the wide use and long research history of Feistel-type structures, its diffusion properties have not been thoroughly analyzed. We tackle this problem in this thesis to unveil the theoretical limitation of the diffusion layers for Feistel-type structures. More specifically, we address mainly three topics in this thesis to improve the diffusion of Feistel-type structures: accurate evaluations for the security of Feistel-type structures regarding the diffusion, efficient design strategies for F-functions of Feistel-type structures, and efficient design strategies for round permutations which are linear permutations between each round.

First, we study the way to precisely evaluate the security of wide variety of BFNs and GFNs against differential and linear cryptanalysis. We propose a new approach to efficiently and accurately evaluate the security of BFNs and GFNs regarding the diffusion with large parameters. Second, we focus on 3-line GFNs. Then, it is proven that 3-line GFNs with double substitution permutation (SP)-functions as F-functions are superior to 4-line GFNs with respect to an efficiency metric for the diffusion. Third, we classify all possible connections of 4-line GFNs, then show that there are only 2 non-contracting constructions in the class of 4-line GFNs up to equivalence, namely, the type-I and type-II GFNs, where 4-line type-I and type-II GFNs have one and two F-functions in a round, respectively. Moreover, we propose to instantiate the GFNs with SPS-functions (two substitution layers separated by a permutation layer) or double SP-functions instead of single SP-functions (one substitution-permutation layer) as F-functions, and show that those constructions are more efficient regarding the diffusion than single SP-functions. Forth, we explore the optimality of BFNs with the wide class of $(\mathrm{SP})^u$ and $(\mathrm{SP})^u\mathrm{S}$ F-functions, where u is an arbitrary positive integer. We provide the tight lower bounds on the minimum number of active S-boxes, which is an important metric for the diffusion, for those constructions, then show that SPS and SPSP F-functions are optimal among $(\mathrm{SP})^u$ and $(\mathrm{SP})^u\mathrm{S}$ constructions in terms of the efficiency metric for the diffusion. Finally, we present how to further improve the diffusion of type-II GFNs by modifying their round permutations (linear permutation between each round). We propose to alternately use

two different round permutations instead of a single round permutation, then show the first optimal constructions for 12-line GFNs which achieve the theoretical lower bound on the maximum diffusion round, another metric for the diffusion.

Our results are useful for a deeper understanding the security and theoretical limitations of Feistel-type symmetric-key cryptosystems. One of the direct applications of our results is designing more efficient and secure symmetric-key primitives.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

1.1.1 Information Security and Cryptography

Information security, a set of practices intended to keep data secure from unauthorized access or alterations, is an essential technology for human society. It mainly ensures confidentiality, integrity and availability of data (also known as the CIA triad), and consists of many technologies including access control, risk management, network security, digital rights management (DRM), anti-malware and certificate authority. Among them, cryptography is a fundamental technology to design a lot of information security applications.

Cryptography provides several important functionalities including authenticity, confidentiality, integrity and randomness. While cryptography has several categories, two fundamental technologies are known as public-key cryptography and symmetric-key cryptography. Public-key cryptography, also referred to as asymmetric-key cryptosystems, was originally developed to remotely and securely share a secret key for a symmetric-key cryptosystem. It basically uses a pair of keys: one is called a public-key, which can be public, and the other is called a secret-key, which must be kept secret. By utilizing its asymmetricity, many interesting and important applications have been developed including a key-sharing and a digital signature. However, in general, a public-key cryptosystem requires a large amount of computations, since it essentially utilizes complicated mathematical problems, namely a trapdoor one-way function. Thus, public-key cryptosystems generally operate far slower than symmetric-key cryptosystems, and this is the main drawback of public-key cryptosystems.

1.1.2 Symmetric-Key Cryptosystems and Block Ciphers

Symmetric-key cryptography including block ciphers, cryptographic hash functions and stream ciphers mainly provides confidentiality and integrity to data. The main advantage of symmetric-key cryptosystems, consisting of iterating weak nonlinear functions, compared to public-key cryptosystems is its computational efficiency. The symmetric-key cryptosystems are necessary for most security applications even when public-key cryptography is used, since they are able to directly treat the large digital data. In fact, symmetric-key cryptosystems are widely used in real-world applications. For instance,

one of the most well-known cryptographic applications TLS (Transport Layer Security) is used everywhere on the web [Res18]. While several options on cryptographic algorithms used in TLS are given, symmetric-key cryptography for data encryption and data hashing is necessary for any options.

It is well-known that the modern cryptography, which is a cryptography not only for military use but also for normal citizen life, started from a development of symmetric-key cryptography DES (Data Encryption Standard) [Nat77]. Since DES was developed, the research on symmetric-key cryptography has been rapidly growing. Findings of a differential attack and a linear attack were two epoch-making discoveries on symmetric-key cryptography [BS91, Mat93]. In fact, a lot of block ciphers were broken by the differential attack or the linear attack. However, those results also opened the new design strategy that ensures the security of block ciphers against those attacks based on theoretical approaches. Thus, the findings of the differential attack and the linear attack are significantly important not only for attackers but also for designers of block ciphers. At the same time, many provable approaches to design a secure block cipher were published. Luby and Rackoff proved that a secure block cipher which is also known as a pseudo random permutation (PRP) is derived from a combination of theoretically secure components which are known as pseudo random functions (PRFs) [LR88]. Their results were improved and extended to the other models [ZMI89a, Pie90, ZMI89b, Mau92]. Nyberg and Knudsen proposed an approach to design a provably secure block cipher against differential attacks, and showed $\mathcal{KN}$-cipher as an instantiation of their approach [NK92]. Then they proved that $\mathcal{KN}$-cipher is provably secure against linear attacks as well [NK95], while it was broken by a higher-order differential attack [JK97, SMK97]. Matsui extended their results to the other structures [Mat96], then proposed a family of block ciphers MISTY as an instantiation [Mat97].

A block cipher, one of symmetric-key primitives, is an n-bit keyed permutation that encrypts and decrypts n-bit digital data by a given k-bit secret key, where n indicates the pre-determined block size (e.g. $n = 64$ or 128) and k denotes the key size. Its direct application is data encryption, and data encryption by a block cipher is used in many security applications. However, a block cipher provides much more functionalities including authenticity and data integrity by using a block cipher as a component known as modes of operation. In fact, it has been well known that NIST standardized several modes of operations including five encryption modes: ECB, CBC, CFB, OFB and CTR, one message authentication mode: CMAC, two authenticated encryption modes: CCM and GCM, and one storage encryption mode: XTS [Nat01b, Nat16, Nat07b, Nat07a, Nat10]. Therefore, if we have a secure and efficient block cipher, we can provide many applications like the above by utilizing those modes of operations.

Moreover, the results on components of block ciphers are directly applied to the other symmetric-key primitives including stream ciphers and cryptographic hash functions, since high-level properties including computational efficiency required for them are similar. In fact, synchronous stream ciphers are constructed from a block cipher using OFB and CTR modes as well as an asynchronous stream cipher from CFB mode. It has also been known that secure cryptographic hash functions are constructed from a secure block cipher referred to as block cipher-based hash functions [PGV93, BRS02]. Thus, it can be considered that a block cipher plays a central role in symmetric-key primitives.

Since Lucifer and the former U.S. standard DES were developed in 1970's, more

than a hundred of modern block ciphers have been proposed including GOST [Nat94], FEAL [SM87, Miy90], Blowfish [Sch93], RC6 [RRY00], MISTY [Mat97], Camellia [AIK+00], AES(Rijndael) [Nat01a] and CLEFIA [SSA+07]. At the same time, a lot of research on designing and analyzing block ciphers have also been published.

A block cipher is typically considered as a class of product ciphers presented by Shannon [Sha49], which combine two or more transformations such as substitution, permutation and modular arithmetic. The concept of the product cipher is that a good combination of simple transformations makes a cipher secure even if those simple transformations themselves are not perfectly secure. Modern block ciphers iteratively utilize such combination, which are known as iterative ciphers. Iterative ciphers iteratively use a round function consisting of nonlinear functions and linear functions. The structures of block ciphers are generally categorized into two structures: Substitution Permutation Networks (SPNs) and Feistel-type structures. SPNs are known as the basic structure of the current U.S. encryption standard AES [Nat01a]. Due to its simplicity and high efficiency, SPNs have been adopted in many block ciphers including SHARK [RDP+96], SQUARE [DKR97], AES [Nat01a], PRESENT [BKL+07] and Midori [BBI+15]. On the other hand, Feistel-type structures including balanced Feistel networks (BFNs) and generalized Feistel networks (GFNs) are the other most widely used structure. Due to its desirable implementation property, it has been also adopted in a lot of block ciphers including DES [Nat77], GOST [Nat94], CAST [Ada97b, Ada97a, AG99], Camellia [AIK+00], CLEFIA [SSA+07] and Piccolo [SIH+11].

1.1.3 Requirements on Block Ciphers

Block ciphers are at least designed to provide sufficient confusion and diffusion which are two important properties identified by Shannon [Sha49]. Confusion means that the ciphertext statistics complicatedly depends on the plaintext statistics so that a cryptanalyst is not able to exploit those statistical properties. Diffusion means that each bit of the plaintext and each bit of the secret key affect a large number of bits of the ciphertext. For modern block ciphers, substitutions typically referred to as substitution-boxes (S-boxes) and permutations including a bit/byte permutation and linear matrix multiplication provide confusion and diffusion, respectively. A good combination of confusion and diffusion is a necessary requirement for designing a secure block cipher.

The security of a block cipher is usually evaluated as computational security. Roughly speaking, a block cipher is considered as computationally secure if there does not exists any distinguisher who distinguishes the block cipher from a random permutation with less computational resources (i.e. time, memory and data) than those required by general attacks including an exhaustive key search. Moreover, since a block cipher generally treats a large number of data, its performance is important as well as its security. However, it has been well known that there is a tradeoff between the security and the performance. Thus, the challenge of designing a good block cipher is building a highly efficient cipher without loosing the security.

As explained, a typical block cipher has an iterative structure, and each iteration called a round function consists of nonlinear functions and linear functions. The confusion of the iterative cipher is provided by nonlinear functions typically known as S-boxes or F-functions. Since, in general, the size of those nonlinear components is not large (e.g. 4-bit

or 8-bit nonlinear permutations), it is feasible to evaluate those security properties by a computer. Moreover, the research on designing a good S-box has been well studied. One of the most well known results is that a good n-bit S-box is derived from an inversion of $\mathrm{GF}(2^n)$ with an appropriate affine transformation [Nyb93, NK95].

We consider that the cipher provides sufficient diffusion when any input bits including the plaintext and the key affect all bits of the ciphertext. In general, the more rounds the iterative cipher has, the better diffusion is provided. Thus, the diffusion property of the cipher is evaluated as the minimum number of rounds achieving the sufficient diffusion. Similarly, if the certain number of nonlinear components is guaranteed to be affected by any input changes, we consider that the cipher provides sufficient diffusion. Therefore, the diffusion property is approximately evaluated as the minimum number of active nonlinear functions (e.g. S-boxes and F-functions), which are nonlinear components affected from any input changes, in each round. Since the faster diffusion leads to smaller number of iterations to be secure and then smaller number of iterations leads to better performance, the diffusion property is crucial for not only security but also the performance of the cipher.

1.2 Motivation

Feistel-type structures including BFNs and GFNs have several desirable implementation properties. One of the most remarkable properties among them is an involution property that does not require an inverse nonlinear function for decryption. Moreover, since only half of the data are updated per one round, each nonlinear function used in Feistel-type structures called an F-function is smaller than that used in SPNs in general. Those properties lead to compact implementation, and thus Feistel-type structures are desirable especially for lightweight cryptography. However, the main drawback of BFNs and GFNs has been known to be slow diffusion compared to SPNs. Thus, the Feistel-type structure generally requires a large number of iterations than an SPN based construction due to its slow diffusion, and it significantly reduces the throughput of the cipher. Despite the wide use of BFNs and GFNs, it is still unclear how to design better diffusion for BFNs and GFNs. We focus on this problem and explore design possibilities of a Feistel-type structure based block cipher. In other words, in this thesis, we try to unveil the theoretical limitation for designing a diffusion of BFNs and GFNs by thoroughly analyzing those diffusions. Our purpose of this thesis is designing a more efficient and secure block cipher. To do so, we deeply analyze the diffusion of Feistel-type structures.

1.3 Related Work and Contributions

In this thesis, in order to improve the diffusion of Feistel-type structures, we consider three main problems: (1) how to more accurately evaluate the lower bounds on the number of active S-boxes for BFNs and GFNs, (2) how to design nonlinear functions called F-function for BFNs and GFNs to improve the diffusion, and (3) how to design more efficient round permutations for GFNs. Note that we investigate the problem (2) separately in three specific Feistel-type structures, namely, 3-line GFNs, 4-line GFNs and BFNs.

First, we treat the problem (1) which focuses on how to more accurately evaluate the diffusion of BFNs and GFNs. It has been known to be complicated to evaluate the lower bounds on the number of active S-boxes for BFNs and GFNs compared to SPNs [DR01]. For BFNs, the work [Kan00] proved the minimum number of active S-boxes in BFNs with SP-functions when the diffusion matrix is the same in all rounds. The papers [SS04, SS06] dealt with the difference cancellation effect for such BFNs and introduced the diffusion switching mechanism which relies on using several distinct diffusion matrices over multiple rounds. The lower bounds on the number of active S-boxes for BFN with SP-functions and multiple-round diffusion were proven in [SP04]. Those for BFNs with SPS-functions and single-round diffusion were analyzed in [Bog10]. For GFNs, lower bounds on the number of active S-boxes were obtained for type-I and type-II GFNs with SP-functions in [WZL06]. Rough lower bounds for type-I and type-II with single SP-functions and multiple-round diffusion were proven by [SA08]. The work [SA08] also provided some numeric analysis for two specific cases of type-I and type-II GFNs with single SP-functions and multiple-round diffusion. While these results significantly improved the security evaluation for BFNs and GFNs with SP-functions, the results only work for small parameter sets of BFNs and GFNs and some of the presented bounds are not tight. We tackle this problem and propose a novel algorithm to more accurately evaluate the minimum number of active S-boxes for BFNs and GFNs with large parameter sets (see **Chapter 4**).

Second, we deal with the problem (2) which concentrates on how to design more efficient nonlinear functions called F-functions used in BFNs and GFNs regarding the proportion of active S-boxes. The design of an F-function significantly affects both the security and the efficiency of BFNs and GFNs. There are several design strategy for F-functions, and those are basically given in the proposed Feistel-type ciphers including DES, Blowfish, MISTY, RC6 and CLEFIA [Nat77, Sch93, Mat97, RRY00, SSA$^+$07]. However, the optimal design strategy with respect to both the security and the efficiency for F-functions in BFNs and GFNs has not been well studied. There were several results on BFNs and GFNs with SP-functions [Kan00, SS04, SS06, WZL06, SA08], and BFNs with SPS-functions were analyzed in [Bog10]. We investigate how to design more efficient BFNs and GFNs by considering several types of SP-type F-functions including not only single SP layer, but also SPS, double SP and more SP layers. We separately analyze three specific types of Feistel-type structures, namely, 3-line GFNs, 4-line GFNs and BFNs for this topic (see **Chapters 5 to 7**).

Finally, we address the problem (3) which focuses on how to design more efficient round permutations which are the other important components in GFNs in terms of diffusion. Since GFNs were proposed in 1980's [ZMI89a], several ciphers using GFNs with cyclic shift as a round permutation have been proposed. However, Suzaki and Minematsu showed that the diffusion property can be improved by modifying a round permutation instead of cyclic shift for type-II GFNs [SM10]. They proposed the best round permutations with respect to the maximum diffusion round, which is one of the metrics for evaluation of diffusion property, for 6- to 16-line type-II GFNs with single round permutations. While it requires huge computations to find good round permutations for large parameters, the search algorithm was improved by [CGT19, DFLM19]. They showed the best single round permutations for 18- to 32- and 36-line type-II GFNs. However, it is still unclear if it is possible to further improve the diffusion by modifying round permuta-

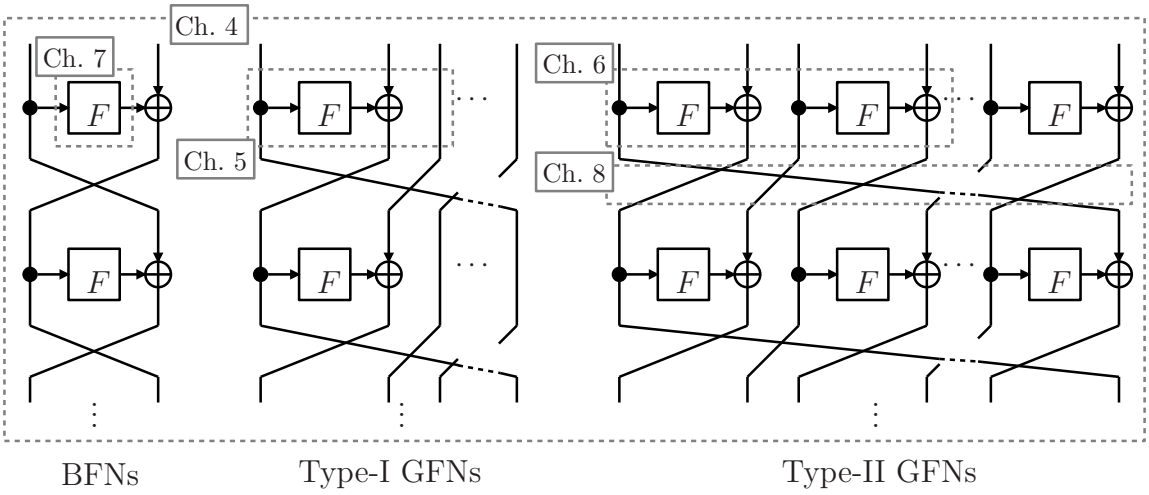

Figure 1.1: Organization of this thesis

tions. We propose to use multiple round permutations alternately instead of single round permutations to further improve the diffusion property (see **Chapter 8**).

We focus on improving the diffusion to design a secure and efficient block cipher in this thesis. However, the opposite design strategy which intentionally utilizes weak and simple components only providing slow diffusion has also been known and studied. While such block ciphers generally require a large number of iterations to be secure, those do not require large computations in each round, e.g., ARX (Addition-Rotation-XOR) design [NW97, BSS+13]. We concentrate on the former design strategy which intends to provide a fast diffusion and do not treat the latter design strategy in this thesis. More detailed explanations on related work are described in each chapter.

1.4 Organization of This Thesis

This thesis consists of nine chapters. The detailed analyses are presented in Chapters 4 to 8, and those research areas are illustrated in Fig. 1.1. We focus on three types of Feistel-type structures which are balanced Feistel networks (BFNs), type-I generalized Feistel networks (type-I GFNs) and type-II generalized Feistel networks (type-II GFNs) depicted in the left, center and right of Fig. 1.1, respectively. The outline of all chapters is summarized as follows:

Chapter 1. Introduction of this thesis. This chapter.

Chapter 2. As preliminaries of this thesis, we explain a structure of block cipher and its security requirements as well as its adversary models and several important attacks.

Chapter 3. We show target structures that we focus on, and evaluation metrics used throughout this thesis.

Chapter 4. We present a new approach to more accurately evaluate the security of wide variety of BFNs and GFNs with respect to the lower bounds on the number of ac-

tive S-boxes. While GFN leads to compact implementations, the security is not well understood, in particular for larger values of the partitioning number which indicates the number of sub-blocks. For both differential and linear cryptanalysis, we first prove tighter lower bounds on the minimum number of active S-boxes for four and six rounds of the GFN utilizing word-based rotation as a round permutation. These bounds are almost twice as large as the previous results in literature [SA08]. Then we present a new approach to derive the first tight lower bounds for the minimum number of active S-boxes in several types of GFN with large parameters. The proposed algorithm utilizes word-based truncated differential search and three-round relations of Feistel connections. By applying our results, the number of rounds required to be secure against differential and linear attacks can be reduced significantly. Moreover, we show that the improved GFN proposed by Suzaki and Minematsu at FSE 2010 have more active S-boxes than the standard GFN (See Ch. 4 in Fig. 1.1).

Chapter 5. We analyze the security of 3-line type-I GFNs. We prove tight lower bounds on the number of differentially and linearly active S-boxes for 3-line GFNs with double SP-functions where two SP-structures are applied one after another and each SP-structure consists of a nonlinear substitution followed by a linear diffusion. We also show 8-round impossible differentials for 3-line GFNs with bijective functions. Moreover, we demonstrate that the proportion of active S-boxes in all S-boxes for such GFNs is by up to 14% higher than that for 4-line GFNs with double SP-functions, when instantiated with MDS matrices. This indicates that the 3-line GFNs can be more efficient in practice than those with 4 lines (See Ch. 5 in Fig. 1.1).

Chapter 6. This chapter deals with the classification, security and efficiency of generalized Feistel networks (GFNs) with 4 lines. We propose a definition of a GFN, essentially limiting consideration to Feistel-type constructions with domain-preserving F-functions and rotation by one line between rounds. Under this definition, we demonstrate that there are only 2 non-contracting representatives in the class of 4-line GFNs up to equivalence, namely, the type-I and type-II GFNs that avoid obvious differential effects. We propose to instantiate the GFNs with SPS-functions (two substitution layers separated by a permutation layer) or double SP-functions (two subsequent substitution-permutation layers) instead of single SP-functions (one substitution-permutation layer only). We prove tight lower bounds on the number of differentially and linearly active functions and S-boxes in such ciphers. Based on these bounds, we show that the instantiation with SPS-functions or double SP-functions using MDS diffusion has a proportion of differentially and linearly active S-boxes by up to 33% and 50% higher than that with single SP-functions for type-I and type-II GFNs, respectively. Moreover, we present the upper bounds on the differential and the linear hull probability for the type-II GFNs with SPS-functions or double SP-functions (See Ch. 6 in Fig. 1.1).

Chapter 7. We explore the optimality of BFNs with SP-type F-functions with respect to their resistance against differential and linear cryptanalysis. Instantiations of BFNs with the wide class of $(\mathrm{SP})^u$ and $(\mathrm{SP})^u\mathrm{S}$ F-functions are considered: One

F-function can contain an arbitrary number of S-box layers interleaved with linear diffusion. For the matrices with maximum diffusion, it is proven that SPS and SPSP F-functions are optimal in terms of the proportion of active S-boxes in all S-boxes – a common efficiency metric for substitution-permutation ciphers. Interestingly, one SP-layer in the F-function is not enough to attain optimality whereas taking more than two S-box layers does not increase the efficiency either (See Ch. 7 in Fig. 1.1).

Chapter 8. We investigate the (im)possibility of further improving the round diffusion of type-II GFNs by modifying the underlying round permutations. First, we generalize a technique called sub-block dividing, which further divides each sub-block into smaller blocks. We prove that the maximum diffusion round of a round permutation with sub-block dividing is four, regardless of the number of sub-blocks. Moreover, we show that the round diffusion of type-II GFNs can be improved by alternately using two different round permutations instead of a single permutation. We present the first results that, by using two round permutations, 10- and 12-line GFNs partially and fully reach the lower bounds on the maximum diffusion round, respectively (See Ch. 8 in Fig. 1.1).

Chapter 9. We conclude this thesis with showing some open problems and ideas for future research.

The main results presented in this thesis have been published in [Shi10, BS11b, BS11a, BS13, SB14, SI22], and they correspond to Chapters 4, 5, 6, 6, 7 and 8, respectively.

Chapter 2

Preliminaries

2.1 Block Ciphers

A block cipher is a keyed permutation consisting of an encryption function $E : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ and decryption function $D : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$. An n-bit ciphertext C is derived from an R-round encryption function E with an n-bit plaintext PT and a k-bit secret key K as follows:

$$CT = E_K(PT).$$

Similarly, an n-bit plaintext PT is calculated from a decryption function D (i.e., the inverse of E) with CT and K as follows:

$$PT = D_K(CT),$$

where $D = E^{-1}$ (See Fig. 2.1).

For modern block ciphers with large n (e.g. $n = 64$ or 128), in general, E has iterative structure. In other words, E consists of a smaller n-bit permutation called a round function $G^{(i)} : \{0,1\}^n \to \{0,1\}^n$, and an output of E is derived from R times $G^{(i)}$ computations with round keys $rk^{(i)}$ generated from K by key scheduling part as follows (See Fig. 2.2):

$$CT = G^{(R)}(...(G^{(2)}(G^{(1)}(P \oplus rk^{(1)}) \oplus rk^{(2)})...) \oplus rk^{(R)}).$$

A block cipher is mainly evaluated by two aspects: security and computational performance. It has been well known that there exists a trade-off between the security and the performance. Designing an extremely high performance but insecure block cipher is meaningless but possible (e.g. E consists of only key XOR as $CT = PT \oplus K$). Similarly to this, it is not hard to design a secure block cipher without having reasonable performance (e.g. E consists of a very complicated nonlinear round function and R is several millions). Therefore, the challenge of designing a good block cipher is building a secure block cipher that is as efficient as possible.

2.2 Security Requirements

The security of cryptography is evaluated in two aspects: information theoretical security and computational security. The information theoretical security was advocated by

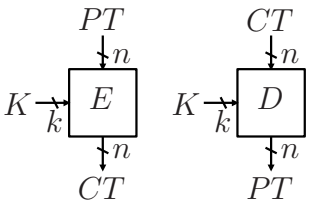

Figure 2.1: Encryption function E and decryption function D

Shannon. For the information theoretically secure block cipher, an adversary is infeasible to distinguish the cipher from a random permutation with a non-negligible probability even if an adversary can use unlimited computational resources. However, the amount of secret key values must be more than that of plaintexts to achieve the information theoretical security. Since such cryptosystem having large secret key values is not realistic, the security of modern block ciphers is usually evaluated by computational security.

The computational security of a block cipher is evaluated by the required resources including computational costs, amount of data and amount of memory to distinguish the cipher from a random permutation under the given adversary model. Roughly speaking, a block cipher is considered to be computationally secure if there does not exist computationally better attacks than general attacks including brute-force attacks.

2.2.1 Adversary Model

We follow the widely accepted concept known as Kerckhoffs's principle: *"a cryptosystem should be secure even if everything about the system, except the key, is public knowledge"* [Ker83]. This principle was reformulated by Shannon as *"the enemy knows the system"* [Sha49]. In other words, a block cipher should be designed to be secure even if an adversary knows everything on the components as long as the secret key is kept secret.

Depending on adversary's capabilities of obtaining and controlling inputs and outputs of an encryption/decryption function, attack settings are mainly classified into the following four scenarios:

Ciphertext-only attack. An adversary is able to obtain randomly chosen ciphertexts.

Known-plaintext attack. An adversary is able to obtain pairs of randomly chosen plaintexts and the corresponding ciphertexts.

Chosen-plaintext attack. An adversary is able to arbitrarily choose plaintexts and obtain the corresponding ciphertexts.

Chosen-ciphertext attack. An adversary is able to arbitrarily choose ciphertexts and obtain the corresponding plaintexts.

Note that chosen data attacks are further classified into non-adaptive model that an adversary chooses data without using the knowledge of the obtained data and adaptive model that an adversary adaptively chooses data depending on the obtained data.

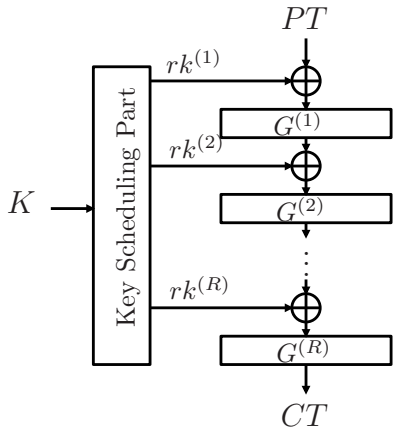

Figure 2.2: Iterative structure

Under those settings, a block cipher is considered to be computationally secure if an adversary, exploiting computation resources less than those required by general attacks, is infeasible to distinguish E from an n-bit random permutation with non-negligible probability. This attack is called distinguishing attack.

While numerous attacks have been proposed for block ciphers, in this thesis, we mainly focus on differential, linear, impossible differential, and saturation attacks which are known as powerful attacks especially for Feistel-type block ciphers.

2.2.2 Brute-Force Attack (General Attack)

The brute-force attack (a.k.a exhaustive key search) on block ciphers is a fundamental attack and is applied to any block ciphers. An attacker requires one known plaintext-ciphertext pair (PT, CT), then encrypts the plaintext PT with possible keys K' as $CT' = E_{K'}(PT)$ until finding K' satisfying $CT' = CT$. This attack requires about 2^k of encryptions, where k is the size of K.

This attack has several variants. In the dictionary attack for a block cipher, an attacker chooses one plaintext PT, then computes and saves the corresponding ciphertexts by all possible keys in advance. Then, the attacker requires one chosen plaintext-ciphertext pair (PT, CT), and find CT from the saved ciphertexts. This attack requires $\mathcal{O}(2^k)$ memory, but requires a few computations in the attack phase. Similarly, time-memory trade-off (TMTO) attack has been known to require $\mathcal{O}(2^{k-t})$ memory and 2^t encryptions.

Those generic attacks are applied to any ciphers including the theoretically ideal cipher. The required resource is approximately estimated as the product of time (i.e., computations) and memory which is about 2^k. Thus, a block cipher is considered to be computationally secure if there does not exist any attacker requiring less than 2^k resources.

2.2.3 Differential Cryptanalysis

A differential cryptanalysis was published in 1990 by Biham and Shamir with applications to DES [BS91]. However, it has been known to the designers of DES at IBM in early 1970s [Cop94]. As the name suggests, the main idea of differential cryptanalysis is to exploit correlations between differences in the inputs and outputs of a block cipher to recover the key. It is a chosen-plaintext attack, in which an attacker is allowed to choose arbitrary plaintexts and obtain the corresponding ciphertexts. The details are given in Section 2.2.8.

2.2.4 Linear Cryptanalysis

A linear cryptanalysis as applied to DES was proposed by Matsui in 1993 [Mat93]. However, similar ideas were published by Shamir [Sha85] in 1985 as well as Tardy-Corfdir and Gilbert [TG91] in 1991. Linear cryptanalysis uses linear approximations of block ciphers to perform key recovery. It is a known-plaintext attack, in which an attacker knows some plaintexts and the corresponding ciphertexts. The details are given in Section 2.2.8.

2.2.5 Impossible Differential Attack

An impossible differential attack [BBS99] exploits an impossible differential which is a differential trail with probability zero, i.e., a differential trail never occurs. It is known as a powerful attack for a block cipher with slow diffusion such as Feistel-type block ciphers. In fact, it has been well known that there exists a trivial impossible differentials on any 5-round BFNs consisting of bijective F-functions.

2.2.6 Saturation Attack

A saturation attack was first proposed by Daemen et al. as a dedicated attack to the block cipher SQUARE [DKR97], then it was generalized by Lucks [Luc01]. It exploits multiset of chosen plaintexts and observes if the sum of a certain part of outputs will be a specific state including a constant and zero. It is also known as a powerful attack for a block cipher with slow diffusion.

2.2.7 Other Attacks

In addition to the above explained powerful attacks especially to a block cipher with slow diffusion, there have been a lot of attacks including differential-linear attack [LH94], boomerang-type attacks (boomerang, amplified boomerang and rectangle attacks [Wag99, KKS00, BDK01]), truncated differential attack [Knu94], truncated linear attack [AIK$^+$00], higher order differential attack [Knu94], interpolation attack [JK97], and meet-in-the-middle attack [BR10].

Evaluating the security of the specific cipher against those attacks is important when we propose a new cipher. However, in this thesis, we focus on higher level of structures of block ciphers to unveil the general strategy for designing a good cipher, and thus we do not treat those dedicated attacks.

2.2.8 Definitions for Differential and Linear Cryptanalysis

For an n-bit function $f : \{0,1\}^n \to \{0,1\}^n$, a differential probability DP_f used in differential cryptanalysis and a linear probability LP_f used in linear cryptanalysis are defined as follows, respectively.

Definition 1 (**Differential probability**). *Given an input difference Δx and an output difference Δy, a differential probability of f is defined as follows:*

$$DP_f(\Delta x, \Delta y) = \Pr_{x \in \{0,1\}^n}(f(x) \oplus f(x \oplus \Delta x) = \Delta y),$$

where $x, \Delta x, \Delta y \in \{0,1\}^n$.

Definition 2 (**Linear probability**). *Given an input linear mask value Γx and an output linear mask value Γy, a linear probability of f is defined as follows:*

$$LP_f(\Gamma x, \Gamma y) = \Big(2 \cdot \Pr_{x \in \{0,1\}^n}\big(x \bullet \Gamma x = f(x) \bullet \Gamma y\big) - 1\Big)^2,$$

where $\bullet$ denotes dot products and x, Γx, $\Gamma y \in \{0,1\}^n$.

The maximum differential probability MDP_f and the maximum differential probability MLP_f are defined as follows:

Definition 3 (**Maximum differential probability**). *The maximum differential probability of f is defined as follows:*

$$MDP_f = \max_{\Delta x \neq 0, \Delta y} DP_f(\Delta x, \Delta y).$$

Definition 4 (**Maximum linear probability**). *The maximum linear probability of f is defined as follows:*

$$MLP_f = \max_{\Gamma x, \Gamma y \neq 0} LP_f(\Gamma x, \Gamma y).$$

A block cipher is considered to be provably secure against differential and linear attacks with parameter q, if MDP_f and MLP_f are 2^{-q} or less, respectively. This approach considering provable security against a differential attack was first shown by Nyberg and Knudsen [NK92, NK95]. Then, it was improved by Aoki and Ohta [AO97]. Matsui presented a new structure considering provable security against differential and linear cryptanalysis [Mat96], then a new block cipher MISTY based on those results was proposed [Mat97].

From the definitions, it requires $\mathcal{O}(2^{2n})$ and $\mathcal{O}(2^{3n})$ times f computations to derive MDP_f and MLP_f. In general, it is computationally feasible to derive MDP_f and MLP_f for small n (e.g. $n = 8$). However, for large n that is usually used in modern block cipher (e.g. $n = 128$), it is almost infeasible to derive those probabilities. Therefore, in order to evaluate the security of modern block ciphers, the maximum differential characteristic probability $MDCP_f$ and the maximum linear characteristic probability $MLCP_f$ are used as approximate values of MDP_f and MLP_f, respectively.

Let a composition of $f_i : \{0,1\}^n \to \{0,1\}^n, i = 1, 2, ..., R$ be $f(x)$ as

$$f(x) = f_R \circ f_{R-1} \circ \cdots \circ f_2 \circ f_1(x).$$

Definition 5 (**Maximum differential characteristic probability**). *The maximum differential characteristic probability of f is defined as follows:*

$$MDCP_f \stackrel{\text{def}}{=} \max_{\substack{\Delta x_0 \neq 0, \\ \Delta x_1, \ldots, \Delta x_R}} \prod_{i=1}^{R} DP_{f_i}(\Delta x_{i-1}, \Delta x_i).$$

Definition 6 (**Maximum linear characteristic probability**). *The maximum linear characteristic probability of f is defined as follows:*

$$MLCP_f \stackrel{\text{def}}{=} \max_{\substack{\Gamma x_0, \ldots, \Gamma x_{R-1}, \\ \Gamma\Gamma x_R \neq 0}} \prod_{i=1}^{R} LP_{f_i}(\Gamma x_{i-1}, \Gamma x_i).$$

It is widely accepted concept that a block cipher E is considered to be practically secure against differential and linear attacks if $MDCP_E$ and $MLCP_E$ are sufficiently low (e.g. less than 2^{-n}) assuming that each differential and linear characteristic is independently and uniformly distributed, respectively.

Chapter 3

Target Structures and Evaluation Metrics

3.1 Target Structures

In this thesis, we focus on a block cipher, one of the symmetric-key primitives. Note that, in general, the results on components of block ciphers are directly applied to the other symmetric-key primitives including stream ciphers and cryptographic hash functions.

While several design strategies have been proposed, Feistel networks and substitution-permutation networks have been central to the design of block ciphers. Balanced Feistel network (BFN), one of the Feistel networks, was adopted in several block ciphers including the former U.S. encryption standard DES [Nat77], GOST [Nat94], Camellia [AIK+00] and KASUMI [Thi99]. Substitution-permutation network (SPN) was also used in a lot of block ciphers including the current U.S. encryption standard AES [Nat01a], PRESENT [BKL+07] and Midori [BBI+15]. At the same time, generalized Feistel network (GFN) was adopted in the U.S. hash function standard SHA-2 and several block ciphers including RC6 [RRY00], CLEFIA [SSA+07] and Piccolo [SIH+11].

3.1.1 Substitution-Permutation Networks (SPNs)

Substitution-permutation networks consist of a substitution layer and a permutation layer in a round (see Fig. 3.1). A substitution layer provides nonlinearity in the cipher consisting of m n-bit nonlinear permutation called S-boxes, which are used in parallel. A permutation layer linearly diffuses the input consisting of an mn-bit linear function. For SPNs, mn-bit plaintext PT is divided into m n-bit inputs $x_0^{(1)}, ..., x_{m-1}^{(1)}$, where $x_j^{(i)} \in \{0,1\}^n$. Then the i-th round output is calculated as follows:

$$(x_0^{(i+1)}|x_1^{(i+1)}|...|x_{m-1}^{(i+1)}) \leftarrow P(S(x_0^{(i)} \oplus k_0^{(i)})|S(x_1^{(i)} \oplus k_1^{(i)})|...|S(x_{m-1}^{(i)} \oplus k_{m-1}^{(i)})),$$

where $k_j^{(i)} \in \{0,1\}^n$ is the j-th round key in the i-th round, $P(\cdot)$ denotes an mn-bit linear function and $s(\cdot)$ denotes an n-bit S-box. Finally, an mn-bit ciphertext CT is derived from R-round outputs $x_0^{(R+1)}, ..., x_{m-1}^{(R+1)}$ as $CT = (x_0^{(R+1)}|x_1^{(R+1)}|...|x_{m-1}^{(R+1)})$.

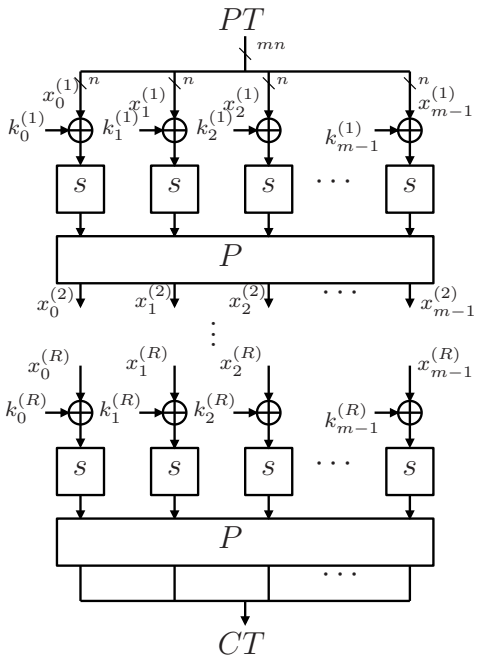

Figure 3.1: Substitution-permutation networks (SPNs)

3.1.2 Balanced Feistel Networks (BFNs)

Balanced Feistel networks was originally used in Lucifer block cipher proposed by Feistel et al. [Fei73]. Then it was adopted in the former U.S. encryption standard DES [Nat77]. After that, BFNs are adopted in a large number of symmetric key primitives, e.g. GOST and KASUMI which is the core of A5/3 cryptosystem in mobile networks [Thi99]. For BFNs, a $2mn$-bit plaintext PT is divided into mn-bit inputs $x_0^{(1)}$ and $x_1^{(1)}$, where $x_j^{(i)} \in \{0,1\}^{mn}$. Then, the i-th round output is calculated as follows:

$$(x_0^{(i+1)}|x_1^{(i+1)}) \leftarrow (x_1^{(i)} \oplus F(x_0^{(i)} \oplus k^{(i)})|x_0^{(i)}),$$

where $k^{(i)} \in \{0,1\}^{mn}$ is the i-th round key and $F^{(i)} : \{0,1\}^{mn} \rightarrow \{0,1\}^{mn}$ is the i-th round function. Finally, a $2mn$-bit ciphertext CT is derived from R-round outputs $x_0^{(R+1)}$ and $x_1^{(R+1)}$ as $CT = (x_1^{(R+1)}|x_0^{(R+1)})$ (see Fig. 3.2).

3.1.3 Generalized Feistel Networks (GFNs)

The formal definition of GFN was given by Zheng et al. [ZMI89b]. For GFNs, a dmn-bit plaintext PT is divided into d sub-blocks (also called as lines), namely, the size of each sub-block is mn-bit. A GFN having d sub-blocks is denoted as GFN$_d$. GFNs are natural extension of BFNs, i.e., BFNs are considered as GFNs with $d = 2$, however, we specifically refer the constructions with $d = 2$ as BFNs, and them with $d > 2$ as GFNs in this thesis. GFNs have several variations depending on its connection of each block and the number of F-functions in each round. Among them, two typical GFNs are called type-I and type-II as shown in Figs. 3.3 and 3.4.

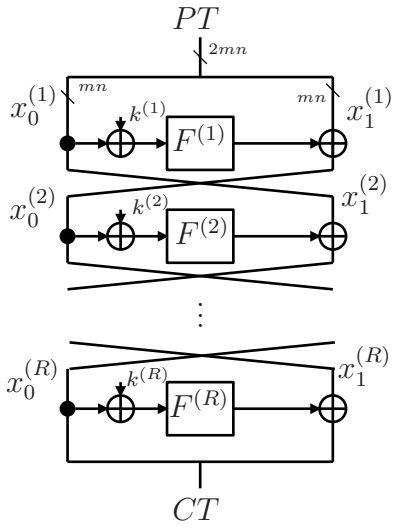

Figure 3.2: Balanced Feistel networks (BFNs)

For type-I GFNs, a dmn-bit plaintext PT is divided into d sub-blocks as $PT = (x_0^{(1)}|x_1^{(1)}|...|x_{d-1}^{(1)})$, where $x_j^{(i)} \in \{0,1\}^{mn}$. Then, the i-th round output is calculated as follows:

$$(x_0^{(i+1)}|x_1^{(i+1)}|...|x_{d-1}^{(i+1)}) \leftarrow (x_1^{(i)} \oplus F^{(i)}(x_0^{(i)} \oplus k^{(i)})|x_2^{(i)}|x_3^{(i)}|...|x_0^{(i)}),$$

where $k^{(i)} \in \{0,1\}^{mn}$ is the i-th round key and $F^{(i)} : \{0,1\}^{mn} \rightarrow \{0,1\}^{mn}$ is the i-th round function. Finally, a dmn-bit ciphertext CT is derived from R-round outputs $x_0^{(R+1)}, ..., x_{d-1}^{(R+1)}$ as $CT = (x_{d-1}^{(R+1)}|x_0^{(R+1)}|...|x_{d-2}^{(R+1)})$ (see Fig. 3.3). Note that Type-I GFNs have one F-function in each round.

For type-II GFNs, a dmn-bit plaintext PT is divided into d sub-blocks as $PT = (x_0^{(1)}|x_1^{(1)}|...|x_{d-1}^{(1)})$, where $x_j^{(i)} \in \{0,1\}^{mn}$. Then, the i-th round output is calculated as follows:

$$(x_0^{(i+1)}|x_1^{(i+1)}|...|x_{d-1}^{(i+1)}) \leftarrow (x_1^{(i)} \oplus F_0^{(i)}(x_0^{(i)} \oplus k_0^{(i)})|x_2^{(i)}|...|x_{d-1}^{(i)} \oplus F_{d/2-1}^{(i)}(x_{d-2}^{(i)} \oplus k_{d/2-1}^{(i)})|x_0^{(i)}),$$

where $k_j^{(i)} \in \{0,1\}^{mn}$ is the j-th round key in the i-th round and $F_j^{(i)} : \{0,1\}^{mn} \rightarrow \{0,1\}^{mn}$ is the j-th round function in the i-th round. Finally, a dmn-bit ciphertext CT is derived from R-round outputs $x_0^{(R+1)}, ..., x_{d-1}^{(R+1)}$ as $CT = (x_{d-1}^{(R+1)}|x_0^{(R+1)}|...|x_{d-2}^{(R+1)})$ (see Fig. 3.4). Note that Type-II GFNs have $d/2$ mn-bit F-functions in each round.

It is well known that Type-II generalized Feistel networks (GFN) [ZMI89b] have several desirable implementation properties, notably compactness. For instance, the GFN has smaller F-functions compared to the balanced Feistel network (BFN) for the same block size. Also GFNs do not need inverse F-functions for decryption, in contrast to Substitution Permutation Networks (SPNs). Recently, lightweight cryptography has become a hot topic. Thus the GFN is an attractive structure for a lightweight symmetric key primitive such as a block cipher or a hash function. This might be one of the reasons why recent block ciphers such as CLEFIA [SSA+07] and HIGHT [HSH+06] utilize the GFN.

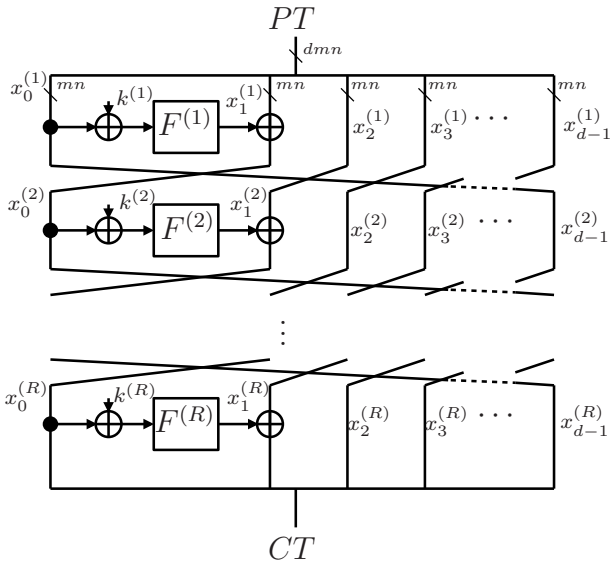

Figure 3.3: Type-I generalized Feistel networks (GFNs)

3.1.4 BFNs and GFNs with SP-Type F-Function

In this thesis, we focus on BFNs and GFNs with SP-type bijective F-functions, that is, with underlying functions whose internal structure is a substitution-permutation network (SPN). An SPN consists of several sequential applications of an S-box layer (S) - several small nonlinear maps applied in parallel - and a diffusion layer (P) - multiplication by a matrix over a binary finite field. The instantiation of a Feistel-type structure with an SP-type F-function is deployed in many cryptographic algorithms including E2 [KMA+00], Twofish [SKW+99], Camellia [AIK+00], CLEFIA [SSA+07], SHAvite-3 [DB09] and Piccolo [SIH+11].

We assume that each round function is the SP-type F-function which consists of m n-bit nonlinear bijective functions called S-boxes and a non-singular $m \times m$ matrix over a chosen field GF(2^n) (see Fig. 3.5). The number of S-boxes in an S-box layer m is also referred to as *bundle size* throughout this thesis.

3.1.5 GFNs with Even-Odd Round Permutation

The standard type-I and type-II GFNs adopt sub-block wise cyclic shift as a round permutation. However, for type-II GFNs, it was proposed by Suzaki and Minematsu [SM10] that the diffusion will be improved by modifying a round permutation instead of cyclic shift. In this thesis, we consider such broader class of round permutation, namely even-odd permutation, where every even-numbered sub-block input is permuted to an odd-numbered output and vice versa by the pre-determined manner. We refer to those constructions as type-II GFNs with even-odd permutations or even-odd shuffles.

For type-II GFNs with even-odd round permutations π, a dmn-bit plaintext PT is divided into d sub-blocks as $PT = (x_0^{(1)}|x_1^{(1)}|...|x_{d-1}^{(1)})$, where $x_j^{(i)} \in \{0,1\}^{mn}$. Then, the

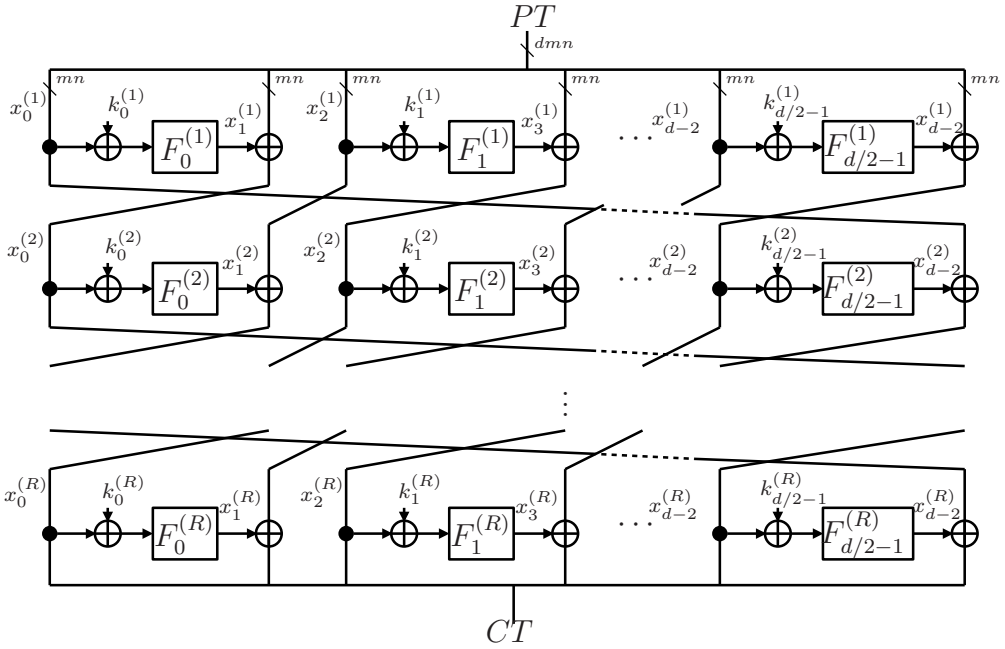

Figure 3.4: Type-II generalized Feistel networks (GFNs)

i-th round output is calculated as follows:

$$(x_0^{(i+1)}|x_1^{(i+1)}|...|x_{d-1}^{(i+1)}) \leftarrow \pi(x_0^{(i)}|x_1^{(i)} \oplus F_0^{(i)}(x_0^{(i)} \oplus k_0^{(i)})|x_2^{(i)}|...|x_{d-2}^{(i)}|x_{d-1}^{(i)} \oplus F_{d/2-1}^{(i)}(x_{d-2}^{(i)} \oplus k_{d/2-1}^{(i)})),$$

where $k_j^{(i)} \in \{0,1\}^{mn}$ is the j-th round key in the i-th round, $F_j^{(i)} : \{0,1\}^{mn} \rightarrow \{0,1\}^{mn}$ is the j-th round function in the i-th round, and $\pi : (\{0,1\}^{mn})^d \rightarrow (\{0,1\}^{mn})^d$ is a deterministic permutation. Since the round permutation π is not applied in the final round, a dmn-bit ciphertext CT is derived from R-round outputs $x_0^{(R+1)}, ..., x_{d-1}^{(R+1)}$ as $CT = \pi^{-1}(x_0^{(R+1)}|...|x_{d-1}^{(R+1)})$ (see Fig. 3.6).

3.2 Evaluation Metrics

In this section, we present evaluation metrics used throughout this thesis.

3.2.1 Active S-Boxes and Active F-Functions

When a key is fixed, only nonlinear functions provide probabilistic behavior in differential and linear cryptanalysis. In other words, the differential probability and linear probability are only reduced by nonlinear functions. We mainly discuss differential cryptanalysis hereafter in this section, however, a similar discussion is also applied to linear cryptanalysis because of its duality [Bih94, Mat94, Kan00].

In order to calculate $MDCP_E$ (the maximum differential characteristic probability of a block cipher E), we need to consider all possible bit differential trails (a.k.a characteristic path). While efficient algorithms to compute such bit characteristics were pro-

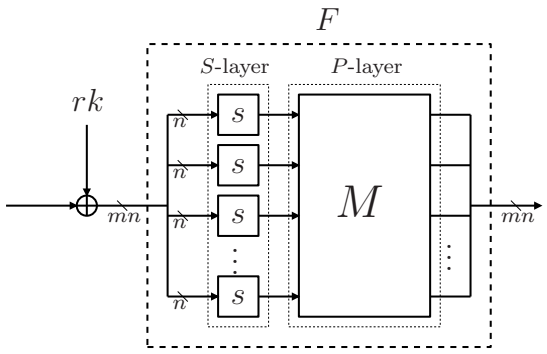

Figure 3.5: SP-type F-function

posed [Mat94], it still requires huge computations. In order to more efficiently evaluate the security against differential cryptanalysis, we search word-wise (a.k.a sub-block wise) truncated differential trails [Knu94] instead of bit differential trails.

Definition 7 (**Truncated differential**). *An n-bit truncated differential $\delta x \in \{0,1\}$ for $\Delta x \in \{0,1\}^n$ is defined as follows:*

$$\delta x = \begin{cases} 0 & (\Delta x = 0), \\ 1 & (\Delta x \neq 0). \end{cases}$$

Each characteristic probability is bounded by the product of the maximum differential (characteristic) probability of all nonlinear functions on the corresponding truncated trails. The maximum differential (characteristic) probabilities of nonlinear components such as S-boxes and F-functions are generally computable or pre-assumed. Therefore, if we exhaustively search all possible truncated differential trails on the cipher, we can compute the upper bound of the maximum differential characteristic probability of E.

When computing the maximum differential characteristic probability by truncated differential search, the number of nonlinear functions on the differential trails is important. Such a nonlinear function having non-zero input difference (or non-zero input linear mask) is referred to as a differentially (or linearly) active function.

Definition 8 (**Active S-boxes and active F-functions**). *A differentially (or linearly) active S-box and active F-function are defined as an S-box and F-function with non-zero input difference (or non-zero input linear mask), respectively.*

Since each active S-box (or F-function) reduces the differential and linear characteristic probabilities, the maximum differential and linear characteristic probabilities are bounded by the minimum number of differentially and linearly active S-boxes (or F-functions), respectively. For example, AES has 16 8-bit S-boxes in a round, and the maximum differential probability of each S-box is known as 2^{-6}. At the same time, the minimum number of active S-boxes for 4-round AES is known as 25 due to wide trail strategy [DR01]. Therefore, the maximum differential characteristic probability of 4-round AES is bounded by $2^{-150}(= (2^{-6})^{25})$. Since the minimum number of active S-boxes is determined by linear functions, it is important metric for evaluations of not

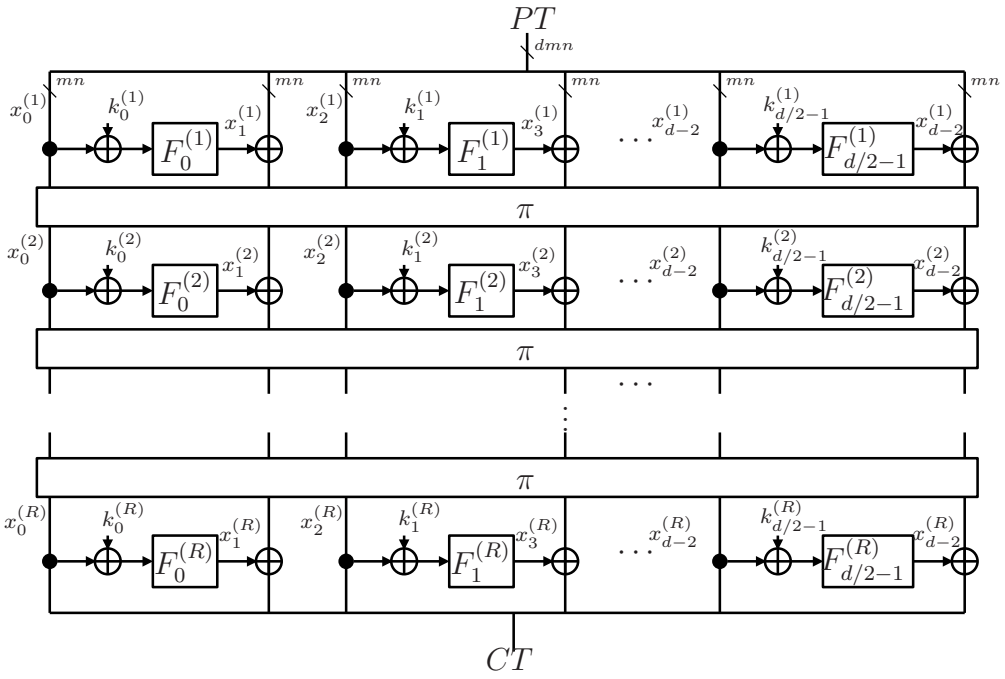

Figure 3.6: Type-II generalized Feistel networks (GFNs) with even-odd round permutation π

only the security against differential cryptanalysis and linear cryptanalysis but also the efficiency of diffusion property.

We give the standard definitions of bundle weight and branch number followed by more specific notations [DR02].

Definition 9 (**Bundle Weight**). *Let $x \in \{0,1\}^{mn}$ be represented as $x = (x_1, x_2, \ldots, x_m)$, where $x_i \in \{0,1\}^n$, then the n-bit bundle weight $w_n(x)$ is defined as*

$$w_n(x) = \sharp\{i | 1 \le i \le m, x_i \neq 0\}. \tag{3.1}$$

Definition 10 (**Branch Number**). *Let $M : \{0,1\}^{mn} \to \{0,1\}^{mn}$. The branch number of M is defined as*

$$\mathcal{B}(M) = \min_{a \neq 0} \{w_n(a) + w_n(M(a))\}. \tag{3.2}$$

We give the definitions of $\mathcal{B}^D$ and $\mathcal{B}^L$ in r-round GFN to show the minimum number of differential and linear active S-boxes, respectively.

Definition 11 (**Differential Branch Number**).

$$\mathcal{B}^D = \min_{1 \le i \le r, 0 \le j \le d/2-1} \mathcal{B}(M_j^{(i)}). \tag{3.3}$$

Definition 12 (**Linear Branch Number**).

$$\mathcal{B}^L = \min_{1 \le i \le r, 0 \le j \le d/2-1} \mathcal{B}({}^tM_j^{(i)}), \tag{3.4}$$

where ${}^tM$ is the transpose matrix of M.

3.2.2 Proportion of Active S-Boxes

A metric has to be defined to enable an efficiency comparison between different designs. The proportion of active S-boxes in all S-boxes is a reasonable efficiency metric with respect to differential and linear cryptanalysis for ciphers based on substitution-permutation. It was introduced in [SP04] by Shirai and Preneel for BFNs and used in [Bog10, Bog11, BS11b, BS11a] for estimating and comparing the efficiency of diverse Feistel constructions, including BFNs.

Both the number of active S-boxes and the number of all S-boxes over several rounds of a BFN depend on the number r of rounds considered and the number m of S-boxes in one F-function.

Definition 13 (**Proportion of active S-boxes $\mathcal{E}_m$ and $\mathcal{E}$**). *The efficiency metric $\mathcal{E}_m(ES)$ is defined as $\mathcal{E}_m(ES) = \lim_{r\to\infty} \frac{\mathcal{NA}_{m,r}(ES)}{\mathcal{NS}_{m,r}(ES)}$, where $\mathcal{NA}_{m,r}(ES)$ is the number of active S-boxes over r rounds and $\mathcal{NS}_{m,r}(ES)$ is the total number of S-box computations over r rounds for a block cipher structure ES when each S-layer consists of m S-boxes in parallel. The number of active S-boxes $\mathcal{NA}_{m,r}$ is measured when the underlying diffusion matrix is MDS, i.e., $\mathcal{B}(M) = m+1$. The efficiency metric $\mathcal{E}$ is defined as $\mathcal{E} = \lim_{m\to\infty} \mathcal{E}_m$.*

Note that this efficiency metric $\mathcal{E}_m$ cannot capture all implementation possibilities and constraints in the field, though it is believed to provide an indication of the efficiency of a block cipher towards the two fundamental types of cryptanalysis, see [SP04, Bog10, Bog11, BS11b, BS11a] for some extensions and discussions with respect to efficiency metrics.

The reason for $\mathcal{E}_m$ being asymptotic in the number of rounds is technical: One can operate with security results without having to extend them to an arbitrary number of rounds. Sometimes, for clarity, it is desirable to compare just two efficiency numbers, which is possible for large blocks (e.g. for hash functions or wide-block encryption) and justifies the usage of $\mathcal{E}$ as an efficiency metric in such cases. The metrics make most sense for tight bounds and iterative trails.

The efficiently metrics $\mathcal{E}$ and $\mathcal{E}_m$ enable us to compare the efficiency of linear diffusion of block cipher structures independent from the block size. For example, by using $\mathcal{E}$ and $\mathcal{E}_m$, it is possible to compare the 3-line GFNs with 4-line GFNs that both consist of the same F-function. It is also possible to compare SPNs with GFNs regarding linear diffusion. For instance, it has been known that an mn-bit SHARK-type SPN construction consisting of a large $m \times m$ MDS matrix as linear function and m n-bit S-boxes has at least $(m + 1)$ active S-boxes every two rounds [RDP+96]. For SHARK-type structure, $\mathcal{NS}_{m,r}(E_{\text{SHARK-type}}) = mr$ and $\mathcal{NA}_{m,r}(E_{\text{SHARK-type}}) = (m + 1)r/2$ when $r = 2, 4, ..., 2u$, where u is a positive integer. Thus, $\mathcal{E}_m(E_{\text{SHARK-type}}) = (m+1)/2m$, then $\mathcal{E}(E_{\text{SHARK-type}}) = 0.5$. This implies that almost half of S-boxes are active for SHARK-type structures. Similarly to this, an m^2n-bit SPN block cipher utilizing wide trail design strategy [DR01] with $m \times m$ MDS matrices and m^2 n-bit S-boxes has been known to have at least $(m + 1)^2$ active S-boxes every four rounds. Therefore, $\mathcal{E}_m(E_{\text{wide-trail}}) = (m + 1)^2/4m^2$, then $\mathcal{E}(E_{\text{wide-trail}}) = 0.25$.

Note that the efficiency metrics $\mathcal{E}_m$ and $\mathcal{E}$ are simplified metrics that explicitly ignore some implementation costs. They ignore the implementation costs of inverse nonlinear functions which are required for SPNs but not required for Feistel-type structures. Moreover, the cost of linear diffusion is also ignored. However, since we aim to compare block

cipher structures including BFNs and GFNs with equal bundle sizes and the same diffusion matrix type, it appears enough to use $\mathcal{E}$ and $\mathcal{E}_m$. We refer to [Bog10] for an extended efficiency metric taking into account the cost of matrix-vector multiplications.

3.2.3 Diffusion Round and Maximum Diffusion Round

As one of the diffusion properties, the maximum diffusion round (DRmax) was defined in [SM10]. This is defined as the minimal number of rounds such that every sub-block of the ciphertext depends on every sub-block of the plaintext. The definitions of the diffusion round (DR) and the maximum diffusion round (DRmax) are given as follows:

Definition 14 (**Diffusion round (*DR*) [SM10]**). *For d-line GFN with round permutation π, diffusion round of the i-th sub-block input $DR_i(\pi)$ is defined as the minimum number of rounds such that the i-th sub-block input is diffused to all output sub-blocks.*

Definition 15 (**Maximum diffusion round (*DRmax*) [SM10]**). *For d-line GFN with round permutation π, the maximum diffusion round $DRmax(\pi)$ is defined as follows:*

$$DRmax(\pi) = \max_{0 \le i < d}(DR_i(\pi)).$$

While DRmax(π) is a simple property efficiently calculated from the given round permutation π, it has a strong relevance to immunity against impossible differential [BBS99] and saturation attacks [DKR97], which are powerful attacks especially for GFN.

Chapter 4

Accurate Evaluation on the Diffusion of Balanced and Generalized Feistel Networks

4.1 Introduction

The GFN divides a plaintext into d sub-blocks, where $d > 2$, instead of $d = 2$ as used in the balanced Feistel networks. The size of the F-functions used in the GFN depends on the partitioning number d and the block size. If the partitioning number d of the GFN is larger, then smaller F-functions will be used. However, a large value of d generally requires a large number of rounds due to its slow diffusion. Hence there is a trade-off between the partitioning number and the required number of rounds. However, this relation has not been clear so far.

Suzaki and Minematsu introduced a GFN with the optimal round permutation with respect to full diffusion property, which is a property that all outputs are affected by all inputs [SM10]. Their paper showed that the improved GFN can be more secure against impossible differential and saturation attacks than the standard GFN. However, they expect that the minimum number of active S-boxes remains about the same. Thus their structures still require at least same number of rounds as the standard GFN to be secure against differential and linear attacks [BS93, Mat93].

It is well understood how to practically evaluate the security against differential and linear attacks by determining the maximum differential and linear characteristic probabilities [DR01, Kan00]. For instance, counting the number of active S-boxes is a well used technique to evaluate the immunity against those attacks [SSA$^+$07]. This approach was used to design many block ciphers and hash functions, including AES [DR02] and Whirlpool [BR11]. In SPN structures, it is relatively easy to evaluate the minimum number of active S-boxes by evaluating the permutation layers as discussed in [DR01]. However, in Feistel structures, this is more complicated due to differential cancellations caused by the XOR operation after the F-function. Kanda showed that the minimum number of active S-boxes of certain consecutive rounds of Feistel structures with SP-type F-function can be represented as the branch number of the matrices used in the structure [Kan00]. Shirai and Araki extended his result to three types of generalized Feistel networks [SA08], which are known as Type-I, Type-II and Nyberg's constructions [Nyb96, ZMI89b]. They

Table 4.1: Summary of our results on the minimum numbers of active S-boxes for each structure, where $\mathcal{B}$ is the differential or the linear branch number of the matrices used in GFN.

rounds	BFN [Kan00, SS06]	$\mathrm{GFN}_d^{\mathrm{std}}$ [SA08]	$\mathrm{GFN}_4^{\mathrm{std}}$ **(this chapter)**	$\mathrm{GFN}_8^{\mathrm{std}}$ **(this chapter)**	$\mathrm{GFN}_6^{\mathrm{imp}}$ **(this chapter)**	$\mathrm{GFN}_8^{\mathrm{imp}}$ **(this chapter)**
4	$\mathcal{B}$	-	$\mathcal{B}+\mathbf{1}$	$\mathcal{B}+\mathbf{1}$	$\mathcal{B}+\mathbf{1}$	$\mathcal{B}+\mathbf{1}$
5	$\mathcal{B}+1$	-	$\mathcal{B}+\mathbf{3}$	$\mathcal{B}+\mathbf{3}$	$\mathcal{B}+\mathbf{3}$	$\mathcal{B}+\mathbf{3}$
6	$\mathcal{B}+2$	$\mathcal{B}+2$	$\mathbf{2}\mathcal{B}+\mathbf{2}$	$\mathbf{2}\mathcal{B}+\mathbf{2}$	$\mathbf{2}\mathcal{B}+\mathbf{2}$	$\mathbf{2}\mathcal{B}+\mathbf{2}$
7	-	-	$\mathbf{2}\mathcal{B}+\mathbf{2}$	$\mathbf{2}\mathcal{B}+\mathbf{4}$	$\mathbf{2}\mathcal{B}+\mathbf{4}$	$\mathbf{2}\mathcal{B}+\mathbf{4}$
8	$2\mathcal{B}+1$	-	$\mathbf{2}\mathcal{B}+\mathbf{3}$	$\mathbf{3}\mathcal{B}+\mathbf{3}$	$\mathbf{4}\mathcal{B}+\mathbf{2}$	$\mathbf{4}\mathcal{B}+\mathbf{3}$
9	$2\mathcal{B}+2$	-	$\mathbf{2}\mathcal{B}+\mathbf{4}$	$\mathbf{3}\mathcal{B}+\mathbf{6}$	$\mathbf{4}\mathcal{B}+\mathbf{4}$	$\mathbf{4}\mathcal{B}+\mathbf{6}$
10	-	-	$\mathbf{3}\mathcal{B}+\mathbf{3}$	$\mathbf{4}\mathcal{B}+\mathbf{5}$	$\mathbf{4}\mathcal{B}+\mathbf{6}$	$\mathbf{5}\mathcal{B}+\mathbf{4}$
11	-	-	$\mathbf{3}\mathcal{B}+\mathbf{5}$	$\mathbf{4}\mathcal{B}+\mathbf{8}$	$\mathbf{4}\mathcal{B}+\mathbf{8}$	$\mathbf{5}\mathcal{B}+\mathbf{7}$
12	$3\mathcal{B}+1$	$2\mathcal{B}+4$	$\mathbf{4}\mathcal{B}+\mathbf{4}$	$\mathbf{6}\mathcal{B}+\mathbf{6}$	$\mathbf{6}\mathcal{B}+\mathbf{2}$	$\mathbf{7}\mathcal{B}+\mathbf{4}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
18	$4\mathcal{B}+4$	$3\mathcal{B}+6$	$\mathbf{6}\mathcal{B}+\mathbf{6}$	$\mathbf{8}\mathcal{B}+\mathbf{8}$	$\mathbf{8}\mathcal{B}+\mathbf{10}$	$\mathbf{10}\mathcal{B}+\mathbf{6}$

showed that any six consecutive rounds of Type-II GFN with any partitioning number have at least the same number of active S-boxes as the BFN. They also introduced an efficient weight-based active S-box search algorithm. However, their algorithm only works for small parameter sets of the GFN and the bound shown in the paper is not tight. Therefore, to design a secure symmetric key primitive, a large number of rounds is still required.

In this chapter, we show the first tight bounds on the minimum number of differential and linear active S-boxes of GFN with large parameter sets. We first prove tight lower bounds for four and six rounds of the standard GFN manually. The obtained bound of six rounds of the standard GFN is almost twice as large as the previous bound. This enables the required number of rounds to be almost halved. Then we show a novel approach to efficiently derive tight lower bounds on the minimum number of active S-boxes of several types of GFN with large parameters including recently proposed GFN utilizing optimal round permutations [SM10]. The proposed algorithm exploits word-based truncated differential search and three-round relations of Feistel connections. By using our results, the required number of rounds to be secure against differential and linear attacks can be reduced significantly. Therefore, our results are useful not only for a deeper understanding the security of GFN, but also for designing an efficient symmetric primitive. Our results in this chapter are summarized in Table 4.1. More detailed results are presented in Tables 4.2 and 4.3.

This chapter is organized as follows. In Section 4.2, definitions and some properties are introduced. In Section 4.3, related work on GFN is explained. Sections 4.4 and 4.5 describe the lower bounds on the number of differential and linear active S-boxes in GFN, respectively. In Section 4.6, we discuss the result obtained in this chapter. Finally, we conclude in Section 4.7.

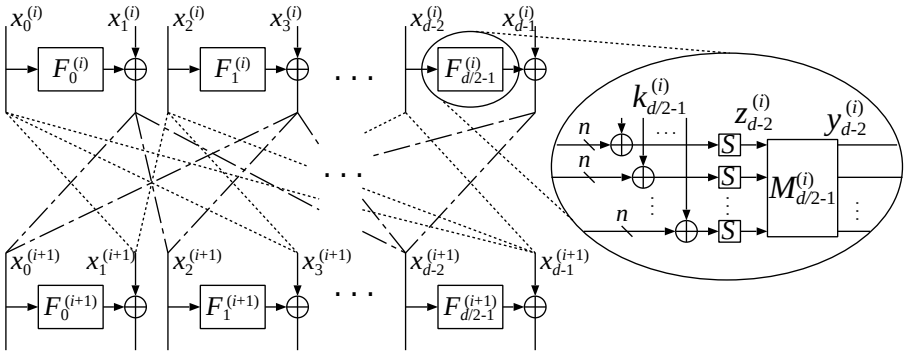

Figure 4.1: GFN_d with SP-type F-function and *even-odd* shuffle

4.2 Preliminaries

4.2.1 Target Structures

In this chapter, we focus on GFN with SP-type F-functions [Kan00] and an *even-odd* shuffle [SM10] as defined in Section 3.1. As a reminder, we show our target structures in Fig. 4.1, where dotted lines show possible connections, each set of outputs and inputs is connected by exactly one line. The sub-diagram on the right in Fig. 4.1 is a zoom in on an F-function. In the figure, $S(\cdot)$ denotes an n-bit bijective S-box and $M_j^{(i)}$ denotes a non-singular $m \times m$ matrix over a chosen field $\mathrm{GF}(2^n)$. $z_{2j}^{(i)}$ and $y_{2j}^{(i)}$ denote an output of the S-boxes and the linear function $M_j^{(i)}$ in $F_j^{(i)}$, respectively. We also restrict π to be a word-based permutation. For instance, π of GFN with the partitioning number eight and the word-based rotation shown in Fig. 4.2 is represented as $\pi(x_0, x_1, ..., x_7) = (x_1, x_2, ..., x_7, x_0)$. We treat several types of π in this chapter. Hereafter $\mathrm{GFN}_d^{\mathrm{std}}$ denotes the GFN_d with the word-based rotation, i.e., standard Type-II GFN, and $\mathrm{GFN}_d^{\mathrm{imp}}$ denotes the GFN_d with the optimal round permutation proposed by Suzaki and Minematsu [SM10][1].

Since each active S-box reduces the differential and linear characteristic probabilities, the maximum differential and linear characteristic probabilities are bounded by the minimum number of differential and linear active S-boxes, respectively. On the other hand, the minimum number of active S-boxes is relevant to the branch number of the linear function. Thus the motivation of this chapter is to clarify the minimum number of differential and linear active S-boxes for GFN by using $\mathcal{B}^D$ and $\mathcal{B}^L$, respectively.

It is well known that the upper bounds on the security against linear attacks are derived from the upper bounds on the security against differential attacks because of its duality [Bih94, Mat94, Kan00]. Thus, in this chapter, we mainly discuss the security against differential attacks. We discuss the security against linear attacks in Section 4.5.

[1]We treat GFN_d with the round permutations No.1 given in Appendix A of [SM10] as $\mathrm{GFN}_d^{\mathrm{imp}}$.

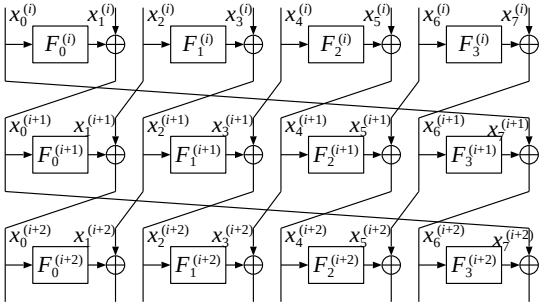

Figure 4.2: $\mathrm{GFN}_8^{\mathrm{std}}$

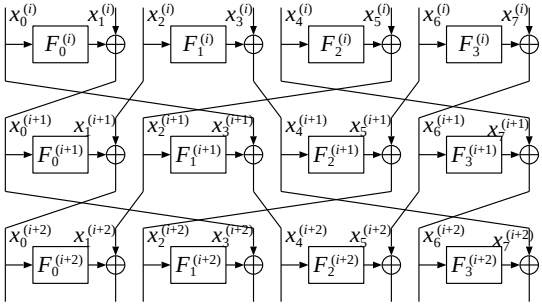

Figure 4.3: $\mathrm{GFN}_8^{\mathrm{imp}}$ [SM10]

4.2.2 Properties of Generalized Feistel Networks

In this section, we present several properties of GFN. As defined in Section 3.2.1, we refer to an F-function which has non-zero input difference or non-zero output mask value as a differential or a linear active F-function, respectively. From the bijectivity of F-functions, the following property holds:

Property 1. *Any two consecutive rounds of GFN have at least one differential active F-function if a non-zero input difference is given.*

We consider the five-round structure of $\mathrm{GFN}_d^{\mathrm{std}}$ shown in Fig. 4.4, and focus on the value $x_{2j}^{(i)}$ in the center of the structure, where $x_{2j}^{(i)}$ and $z_{2j}^{(i)}$ denote an input of $F_j^{(i)}$ and an output of S-boxes in $F_j^{(i)}$, respectively. Let $D_j^{(i)}$ denote the number of differential active S-boxes in $F_j^{(i)}$. Since all S-boxes are bijective, we have the following relations.

Property 2.

$$D_j^{(i)} = w_n(\Delta x_{2j}^{(i)}) = w_n(\Delta z_{2j}^{(i)}). \tag{4.1}$$

Then the following property is derived [SA08].

Property 3 (**Three-round relation of Feistel connection**). *If $D_j^{(i)} \neq 0$, then $D_j^{(i)} + D_{j+1}^{(i-1)} + D_{j+1}^{(i+1)} \geq \mathcal{B}^D$.*

Proof.

$$M_j^{(i)}(\Delta z_{2j}^{(i)}) = \Delta x_{2(j+1)}^{(i-1)} \oplus \Delta x_{2(j+1)}^{(i+1)}. \tag{4.2}$$

From the definition of $\mathcal{B}^D$, $w_n(\Delta z_{2j}^{(i)}) + w_n(M_j^{(i)}(\Delta z_{2j}^{(i)})) \geq \mathcal{B}^D$ if $\Delta z_{2j}^{(i)} \neq 0$. Also, $w_n(a) + w_n(b) \geq w_n(a \oplus b)$ holds, then we have

$$w_n(\Delta z_{2j}^{(i)}) \neq 0 \Rightarrow w_n(\Delta z_{2j}^{(i)}) + w_n(\Delta x_{2(j+1)}^{(i-1)}) + w_n(\Delta x_{2(j+1)}^{(i+1)}) \geq \mathcal{B}^D. \tag{4.3}$$

□

In this chapter, we refer to this relation of three values $\Delta x_{2j}^{(i)}$, $\Delta x_{2(j+1)}^{(i-1)}$ and $\Delta x_{2(j+1)}^{(i+1)}$ as the three-round relation of the Feistel connection. The following properties are also obtained.

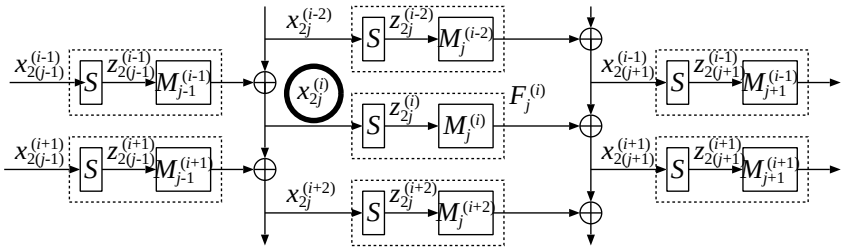

Figure 4.4: Five rounds of $\mathrm{GFN}_d^{\mathrm{std}}$ (untwisted form)

Property 4. *If* $D_j^{(i)} \neq 0$, *then* $D_{j-1}^{(i-1)} + D_j^{(i-2)} \geq 1$, $D_{j-1}^{(i+1)} + D_j^{(i+2)} \geq 1$, *and* $D_{j+1}^{(i-1)} + D_{j+1}^{(i+1)} \geq 1$.

Proof.

$$M_{j-1}^{(i-1)}(\Delta z_{2(j-1)}^{(i-1)}) \oplus \Delta x_{2j}^{(i-2)} = \Delta x_{2j}^{(i)} \neq 0, \tag{4.4}$$

$$M_{j-1}^{(i-1)}(\Delta z_{2(j-1)}^{(i-1)}) \neq \Delta x_{2j}^{(i-2)}. \tag{4.5}$$

Then $M_{j-1}^{(i-1)}(\Delta z_{2(j-1)}^{(i-1)})$ and $\Delta x_{2j}^{(i-2)}$ cannot be 0 simultaneously. Thus, $D_{j-1}^{(i-1)} + D_j^{(i-2)} \geq 1$. The other properties can be proved in a similar way. □

We give some definitions of round permutations to use three-round relation of the Feistel connections in GFN. Let π_E, π_O be index mappings. π_E is the index mapping of π from even numbered blocks to odd-number blocks and all indexes are divided by two. For example, π_E of $\mathrm{GFN}_8^{\mathrm{std}}$ shown in Fig. 4.2 is represented as $\pi_E[0] = 3$, $\pi_E[1] = 0$, $\pi_E[2] = 1$ and $\pi_E[3] = 2$. Similarly, π_O is the index mapping of π from odd numbered blocks to even-number blocks and all indexes are divided by two. For example, π_O of $\mathrm{GFN}_8^{\mathrm{std}}$ is the identity mapping, and π_O of $\mathrm{GFN}_8^{\mathrm{imp}}$ is represented as $\pi_O[0] = 0$, $\pi_O[1] = 2$, $\pi_O[2] = 1$ and $\pi_O[3] = 3$. By using these mappings π_E and π_O, the three-round relations of the Feistel connections in GFN can easily be represented. For instance, the three F-functions input differences $\Delta x_{2\pi_E^{-1}[j/2]}^{(i)}$, $\Delta x_j^{(i+1)}$ and $\Delta x_{2\pi_O[j/2]}^{(i+2)}$ in Figs. 4.2 and 4.3 satisfy the three-round relation shown in Property 3 independently, where $j = \{0, 2, 4, 6\}$ and π_E^{-1} is an inverse mapping of π_E.

Let $\Delta \boldsymbol{x}^{(i)} = (\Delta x_0^{(i)}, \Delta x_2^{(i)}, ..., \Delta x_{d-2}^{(i)})$. Then the following property is derived.

Property 5. *Any three consecutive rounds of* $(i-1)$ *to* $(i+1)$*-round of* GFN_d *have at least* $w_{mn}(\Delta \boldsymbol{x}^{(i)}) \cdot \mathcal{B}^D$ *differential active S-boxes, specifically,*

$$\sum_{s=0}^{d/2-1} \sum_{t=i-1}^{i+1} D_s^{(t)} \geq w_{mn}(\Delta \boldsymbol{x}^{(i)}) \cdot \mathcal{B}^D. \tag{4.6}$$

Proof. From the definition of the *even-odd* shuffle, each i-th round output after the XOR operation is mapped to the corresponding F-function of $(i-1)$-th round and $(i+1)$-th round respectively. In other words, there exist d independent three-round relations shown in Property 3. Thus the number of active S-boxes in three consecutive rounds is bounded by the bundle weight of the differentials in the center. □

The mappings π_E, π_O, and the Property 5 are useful to evaluate the minimum number of active S-boxes of GFN.

4.3 Related Work

In this section, we discuss previous results related to GFN. The formal definition of GFN was given by Zheng et al. [ZMI89b]. Several cryptographic properties of these structures were analyzed in [KHS+03, MV00]. Provable security of $\mathrm{GFN}_4^{\mathrm{std}}$ against differential and linear attacks was discussed by Lee et al. [LKS+06]. In their results, more than five rounds of $\mathrm{GFN}_4^{\mathrm{std}}$ have the maximum differential probability $p^4 + 2p^5$ and the maximum linear probability $q^4 + 2q^5$, where p and q are the maximum average differential probability and the maximum average linear probability of the F-functions used in the structure, respectively.

The practical security of $\mathrm{GFN}_d^{\mathrm{std}}$ against differential and linear attacks was discussed by Shirai and Araki [SA08]. They showed the lower bounds on the number of active S-boxes in three types of generalized Feistel networks, Type-I, Type-II and Nyberg's constructions [Nyb96, ZMI89b]. In their results, any six consecutive rounds of $\mathrm{GFN}_d^{\mathrm{std}}$ have at least $\mathcal{B}^D + 2$ active S-boxes[2]. Moreover, they introduced efficient weight-based active S-box search algorithms that can derive the minimum number of active S-boxes of GFN. Though their algorithm is efficient, still a large computation is required to evaluate large parameter sets of GFN, namely, it requires to search at most $(m+1)^{d(r+1)/2}$ values to evaluate r-round $\mathrm{GFN}_d^{\mathrm{std}}$. Thus the algorithm does not work for $\mathrm{GFN}_d^{\mathrm{std}}$ with large parameters. We use this algorithm to verify the tightness of our results in Section 4.4.4.

Suzaki and Minematsu discussed round permutations of GFN [SM10]. They mainly focused on full diffusion property, which is a property that all outputs are affected by all inputs. They showed that the diffusion property of the GFN_d ($d > 4$) could be better than $\mathrm{GFN}_d^{\mathrm{std}}$ by replacing its round permutation from the word-based rotation used in $\mathrm{GFN}_d^{\mathrm{std}}$. In their chapter, although the improved GFN has better properties with respect to full diffusion, they have about the same number of active S-boxes[3] as $\mathrm{GFN}_d^{\mathrm{std}}$.

4.4 Differential Active S-boxes in GFN

In this section, we present the minimum number of differential active S-boxes in several types of GFN. First, we show better lower bounds for four and six rounds of $\mathrm{GFN}_d^{\mathrm{std}}$. Then, we introduce an exhaustive search algorithm that determines the minimum number of differential active S-boxes for all types of GFN efficiently. By using this algorithm, we present several lower bounds on GFN. Finally, we compare the results obtained from the new algorithm with the results obtained from weight-based exhaustive active S-box search to verify the tightness of the new bounds.

[2]Their results were given by $\mathcal{B}^D$, and $\mathcal{B}_2^D$ which is a branch number of two consecutive matrices. If matrices used in each F-function are different, $\mathcal{B}_2^D$ can be more than two. However, in our model, $\mathcal{B}_2^D = 2$.

[3]Note that, they evaluated the number of active S-boxes by counting the number of active F-functions as active S-boxes.

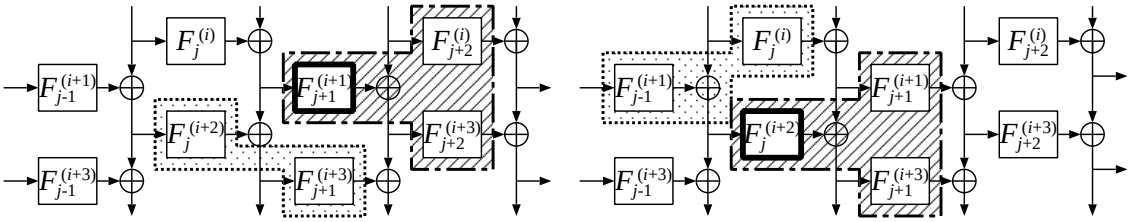

Figure 4.5: Four rounds of $\mathrm{GFN}_d^{\mathrm{std}}$ (untwisted form)

4.4.1 The Lower Bounds for Four and Six Rounds of $\mathrm{GFN}_d^{\mathrm{std}}$

Theorem 1. *Let $d \geq 4$. Any four consecutive rounds of GFN_d^{std} have at least $\mathcal{B}^D + 1$ differential active S-boxes.*

Proof. We consider four consecutive rounds that start from the i-th round as described in Fig. 4.5. From Property 1, there is at least one active F-function in any two consecutive rounds, i.e., there is at least one active F-function in the $(i+1)$-th round or the $(i+2)$-th round. As shown on the left side of Fig. 4.5, suppose that the j-th F-function in the $(i+1)$-th round is active, namely, $D_j^{(i+1)} \neq 0$. In that case, $D_{j+1}^{(i+1)} + D_{j+2}^{(i)} + D_{j+2}^{(i+3)} \geq \mathcal{B}^D$ from Property 3, and $D_j^{(i+2)} + D_{j+1}^{(i+3)} \geq 1$ from Property 4. Thus these four rounds have at least $\mathcal{B}^D + 1$ differential active S-boxes. Similarly, in the case of an active F-function in the $(i+2)$-th round, we have the same bound as shown in the right side of Fig. 4.5. Therefore, we obtain $\Sigma_{s=0}^{d/2-1}\Sigma_{t=i}^{i+3} D_s^{(t)} \geq \mathcal{B}^D + 1$. □

Theorem 2. *Let $d \geq 4$. Any six consecutive rounds of GFN_d^{std} have at least $2\mathcal{B}^D + 2$ differential active S-boxes.*

Proof. We consider six consecutive rounds that start from the i-th round. From Property 1, there is at least one active F-function in any two consecutive rounds, i.e., there is at least one active F-function in the $(i+2)$-th round or the $(i+3)$-th round. Suppose that the j-th F-function in the $(i+2)$-th round is active, i.e., $D_j^{(i+2)} \neq 0$ as shown in Fig. 4.6. Then we consider the following cases.

Case 1. If $D_{j+1}^{(i+3)} = 0$, then $D_{j+1}^{(i+1)} \neq 0$ from Property 4 , also $D_j^{(i)} + D_{j-1}^{(i+1)} \geq 1$ and $D_{j-1}^{(i+3)} + D_j^{(i+4)} \geq 1$. Then $D_{j+1}^{(i+1)} + D_{j+2}^{(i)} + D_{j+2}^{(i+2)} \geq \mathcal{B}^D$ from the fact $D_{j+1}^{(i+1)} \neq 0$ and Property 3. We then consider the following two cases.

Case 1-1. If $D_j^{(i+4)} \neq 0$, then $D_j^{(i+4)} + D_{j+1}^{(i+5)} \geq \mathcal{B}^D$ from Property 3. Thus we have $\Sigma_{s=0}^{d/2-1}\Sigma_{t=i}^{i+5} D_s^{(t)} \geq 2\mathcal{B}^D + 2$.

Case 1-2. If $D_{j-1}^{(i+3)} \neq 0$, then $D_{j-1}^{(i+3)} + D_j^{(i+2)} + D_j^{(i+4)} \geq \mathcal{B}^D$ from Property 3 and $D_{j-2}^{(i+4)} + D_{j-1}^{(i+5)} \geq 1$ from Property 4. Thus we obtain $\Sigma_{s=0}^{d/2-1}\Sigma_{t=i}^{i+5} D_s^{(t)} \geq 2\mathcal{B}^D + 2$.

Case 2. $D_{j+1}^{(i+3)} \neq 0$, then $D_{j+2}^{(i+2)} + D_{j+2}^{(i+4)} \geq 1$. Then we consider the following cases.

Case 2-1. If $D_{j+2}^{(i+2)} \neq 0$, then $D_{j+3}^{(i+1)} + D_{j+3}^{(i+3)} \geq 1$. We consider the following two cases.

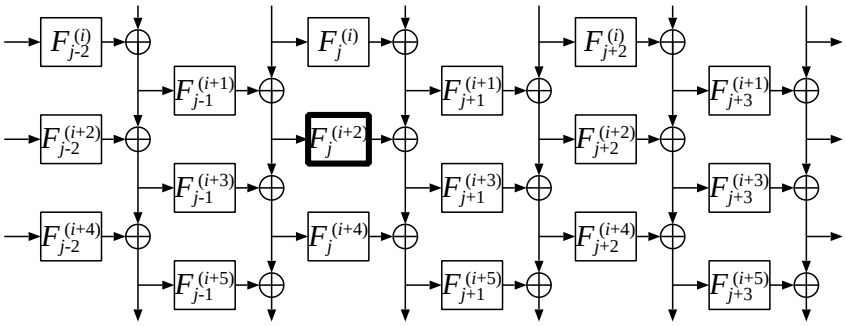

Figure 4.6: Six rounds of $\mathrm{GFN}_d^{\mathrm{std}}$ (untwisted form)

Case 2-1-1. If $D_{j+3}^{(i+1)} \neq 0$, then $D_{j+3}^{(i+1)} + D_{j+4}^{(i)} + D_{j+4}^{(i+2)} \geq \mathcal{B}^D$. Also, $D_{j+1}^{(i+3)} + D_{j+2}^{(i+2)} + D_{j+2}^{(i+4)} \geq \mathcal{B}^D$, $D_{j+1}^{(i+1)} + D_{j+2}^{(i)} \geq 1$, and $D_{j}^{(i+4)} + D_{j+1}^{(i+5)} \geq 1$. Therefore, we have $\Sigma_{s=0}^{d/2-1}\Sigma_{t=i}^{i+5} D_s^{(t)} \geq 2\mathcal{B}^D + 2$.

Case 2-1-2. If $D_{j+3}^{(i+3)} \neq 0$, then $D_{j+2}^{(i+4)} + D_{j+3}^{(i+5)} \geq 1$. Also, $D_{j}^{(i+2)} + D_{j+1}^{(i+1)} + D_{j+1}^{(i+3)} \geq \mathcal{B}^D$, $D_{j+2}^{(i+2)} + D_{j+3}^{(i+1)} + D_{j+3}^{(i+3)} \geq \mathcal{B}^D$, and $D_{j}^{(i+4)} + D_{j+1}^{(i+5)} \geq 1$. Thus, we obtain $\Sigma_{s=0}^{d/2-1}\Sigma_{t=i}^{i+5} D_s^{(t)} \geq 2\mathcal{B}^D + 2$.

Case 2-2. If $D_{j+2}^{(i+4)} \neq 0$, then $D_{j+2}^{(i+4)} + D_{j+3}^{(i+3)} + D_{j+3}^{(i+5)} \geq \mathcal{B}^D$. Also, $D_{j}^{(i+2)} + D_{j+1}^{(i+1)} + D_{j+1}^{(i+3)} \geq \mathcal{B}^D$, $D_{j-1}^{(i+1)} + D_{j}^{(i)} \geq 1$, and $D_{j}^{(i+4)} + D_{j+1}^{(i+5)} \geq 1$. Therefore, we have $\Sigma_{s=0}^{d/2-1}\Sigma_{t=i}^{i+5} D_s^{(t)} \geq 2\mathcal{B}^D + 2$.

Considering all cases, we conclude that any six consecutive rounds in $\mathrm{GFN}_d^{\mathrm{std}}$ have at least $2\mathcal{B}^D + 2$ differential active S-boxes when there is at least one active F-function in the $(i+2)$-th round. Similarly, in the case that there exists at least one active F-function in the $(i+3)$-th round, we have the same bound. Finally, we conclude that any six consecutive rounds in $\mathrm{GFN}_d^{\mathrm{std}}$ have at least $2\mathcal{B}^D + 2$ differential active S-boxes. □

All cases used for this proof of the minimum number of active S-boxes in six rounds of $\mathrm{GFN}_4^{\mathrm{std}}$ are shown in Figs. 4.7-4.11. In these figures, the F-function indicated by the bold line is determined to be active and the F-function indicated by the dotted line is determined to be non-active. Also, there is at least one active S-box in the area encircled by dotted line, and there are at least $\mathcal{B}^D$ active S-boxes in the area encircled by chain line.

The bound given by this theorem is almost twice as large as the previous result. Thus, the required number of rounds of $\mathrm{GFN}_d^{\mathrm{std}}$ to be secure against differential attacks can be almost halved by using this bound.

While it might be possible to prove the minimum number of active S-boxes of a large number of rounds of $\mathrm{GFN}_d^{\mathrm{std}}$ in a similar way, such proofs would be quite complex when the number of rounds is large. In other words, the number of cases to be considered would be increased drastically. Also, using the approaches so far, the relation between the partitioning number d and the minimum number of active S-boxes is still unclear. If all possible cases are checked efficiently, the minimum number of active S-boxes of the

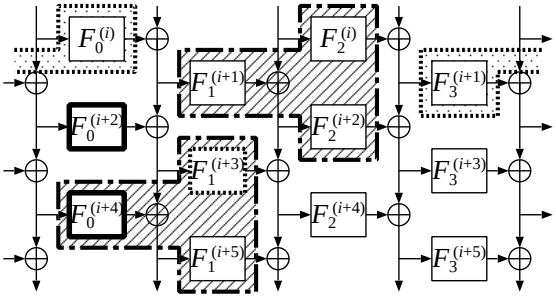

Figure 4.7: Case 1-1

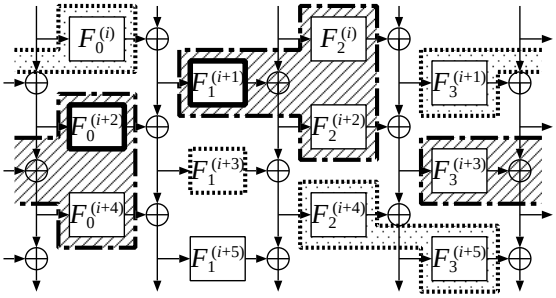

Figure 4.8: Case 1-2

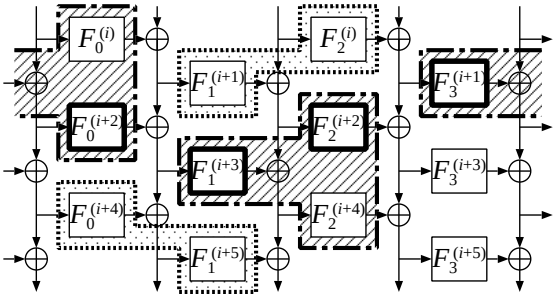

Figure 4.9: Case 2-1-1

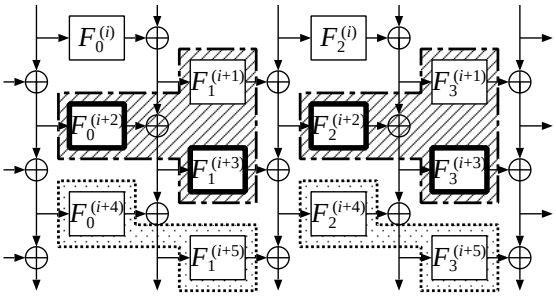

Figure 4.10: Case 2-1-2

structures can be derived easily. Therefore, we propose another approach to efficiently derive the minimum number of active S-boxes of GFN with large parameter sets in the following section.

4.4.2 The Search for the Minimum Number of Differential Active S-Boxes

In this section, we introduce the search algorithm of the minimum number of differential active S-boxes for GFN. This algorithm consists of the following two steps: (a) searching active F-function paths of GFN exhaustively by word-based truncated differential search, (b) determining the minimum number of differential active S-boxes from a given path.

Let $X^{(i)} \in \{0,1\}^{d/2}$ be the input differences of the mn-bit truncated differentials of the i-th F-function, i.e., $X^{(i)} = (w_{mn}(\Delta x_0^{(i)}), w_{mn}(\Delta x_2^{(i)}), ..., w_{mn}(\Delta x_{d-2}^{(i)}))$, where $X^{(0)}$ is the first input differences to XOR operation side, namely, $X^{(0)} = (w_{mn}(\Delta x_1^{(1)}), w_{mn}(\Delta x_3^{(1)}), ..., w_{mn}(\Delta x_{d-1}^{(1)}))$. Let $\mathrm{BD}(R)$ be the minimum number of differential active S-boxes in R-round GFN, then $\mathrm{BD}(R)$ is calculated as follows:

Step 1. Initialize $\mathrm{BD}(R)$ to a sufficiently large value, such as the total number of S-boxes.

Step 2. Choose a possible active F-function path by searching mn-bit truncated differential paths of GFN. First, $X^{(0)}$ and $X^{(1)}$ are chosen exhaustively. Then, i-th round truncated differential path $X^{(i)}$ $(i \geq 3)$ can be determined by $X^{(i-2)}$ and $X^{(i-1)}$ as follows:

$$X_j^{(i)} = \begin{cases} X^{(i-1)}_{\pi_O^{-1}[j]} \oplus X^{(i-2)}_{\pi_E^{-1}[\pi_O^{-1}[j]]} & , \quad \text{if } X^{(i-1)}_{\pi_O^{-1}[j]} \wedge X^{(i-2)}_{\pi_E^{-1}[\pi_O^{-1}[j]]} = 0, \\ 0, 1 & , \quad \text{otherwise,} \end{cases}$$

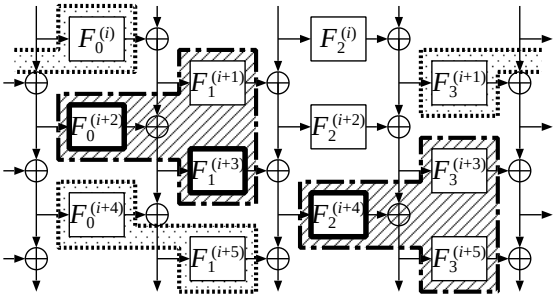

Figure 4.11: Case 2-2

where $X_j^{(i)}$ is a j-th bit of $X^{(i)}$ and $X_0^{(i)}$ is the most significant bit of $X^{(i)}$. In the case of $i = 2$, $X^{(i-2)}_{\pi_E^{-1}[\pi_O^{-1}[j]]}$ is replaced by $X^{(i-2)}_{\pi_O^{-1}[j]}$. Thus R-round path of $X^{(i)}(0 \leq i \leq R)$ is calculated by using the previous algorithm repeatedly.

Step 3. Determine the minimum number of active S-boxes from a given truncated differential path. This step is described in Fig. 4.12. If the bound obtained from the algorithm Fig. 4.12 is less than BD(R), then BD(R) is updated. The detailed explanation of this step is presented in the following section.

Step 4. If all possible truncated differential paths have been checked, terminate the program. Otherwise, go to Step 2.

We give an improvement of Step 2. From Property 5, it is easy to derive a rough bound on the number of $\mathcal{B}^D$ in the structure by checking some Hamming weights of $X^{(i)}$. Then if the obtained rough bound is more than the current bound BD(R), we can simply skip this path. For example, in the case of $R = 6$, we check max(Hw($X^{(2)}$)+ Hw($X^{(5)}$), Hw($X^{(3)}$), Hw($X^{(4)}$)), where Hw(X) denotes a Hamming weight of X. This improvement results in a speed-up in practice.

4.4.3 Detailed Explanation of the Algorithm

We explain the algorithm presented in the previous section in detail. The most important part of this algorithm is Step 3. In this step, we focus on three-round relations in GFN. As discussed in Section 4.2.2, we find three-round relations in any three consecutive rounds by using π_E^{-1} and π_O. Then we count the number of $\mathcal{B}^D$ in GFN greedily from top to bottom. Finally, we count the remaining constants in the structure. We exploit fact that there exist $d/2$ independent three-round relations in any three consecutive rounds of GFN$_d$ and these relations can be obtained by using the mappings π_E^{-1} and π_O. Once $d/2$ independent three-round relations are obtained, the number of $\mathcal{B}^D$ in three consecutive rounds is easily derived from Property 3 and 5. However, in this algorithm, there should be some overlapping values. To avoid this problem, we use a flag for each bit of truncated differentials. Once a value is used for counting the number of $\mathcal{B}^D$ in the certain three consecutive rounds, then the flag is set. Then this value cannot be used twice, and the algorithm works correctly.

Note that the comparison phase in Step 3 depends on the value of $\mathcal{B}^D$. Suppose that the current BD(R) = $2\mathcal{B}^D$, and a new value of $\mathcal{B}^D + 3$ is obtained. In that case, the

Algorithm $CountBD(r, X^{(1)}, ..., X^{(r)})$ **:**
Clear flags of $X_j^{(i)}, (1 \le i \le r, 0 \le j \le d/2-1)$
$S = 0$
for $i \leftarrow 2$ to $(r-1)$ do
  for $j \leftarrow 0$ to $(d/2-1)$ do
    if $(X_j^{(i)} = 1) \wedge$ (flags of $X^{(i-1)}_{\pi_E^{-1}[j]}$ and $X_j^{(i)}$ are not set) then
      $S \leftarrow S + 1$
      Set flags of $X_j^{(i)}$, $X^{(i-1)}_{\pi_E^{-1}[j]}$ (if $X^{(i-1)}_{\pi_E^{-1}[j]} = 1$), and $X^{(i+1)}_{\pi_O[j]}$ (if $X^{(i+1)}_{\pi_O[j]} = 1$)
$T = 0$
for $i \leftarrow 1$ to r do
  for $j \leftarrow 0$ to $(d/2-1)$ do
    if $X_j^{(i)} = 1 \wedge$ (flag of $X_j^{(i)}$ is not set) then
      $T \leftarrow T + 1$
return $S \cdot \mathcal{B}^D + T$

Figure 4.12: Algorithm $CountBD(r, X^{(0)}, ..., X^{(r)})$.

BD(R) is updated when $\mathcal{B}^D > 2$, because $2\mathcal{B}^D \le \mathcal{B}^D + 3$. However, when $\mathcal{B}^D = 2$, it should not be updated. This chapter contains results for $\mathcal{B}^D > 2$.

We now show that this algorithm does not always give the best bound in the structure from a given path. The path in the left of Fig. 4.13 is the case, where an F-function indicated by bold line is determined to be active and an F-function indicated by dotted line is determined to be non-active. In this case, the algorithm (Fig. 4.12) outputs $\mathcal{B}^D + 4$ instead of $2\mathcal{B}^D + 2$ as the path in the center of Fig. 4.13, where there is at least $\mathcal{B}^D$ active S-boxes in the area encircled by chain line. However, because the purpose of this algorithm is to find a lower bound on the number of differential active S-boxes, the best bound in this step is not necessary. We can avoid this problem by adding search patterns to the algorithm. For example, if we compute the bound both way, i.e., from top to bottom and from bottom to top, the algorithm outputs the best bound from the path at the right of Fig. 4.13. However, from our calculations, it seems that this change does not provide an improvement in practice. In other words, the obtained lower bound is the same even if we add some search patterns to the algorithm, e.g., the path in Fig. 4.13 is not the minimum path for $\mathrm{GFN}_4^{\mathrm{std}}$.

4.4.4 Comparison of Results

We verified the tightness of the obtained lower bounds by comparing with the results obtained by the weight-based exhaustive active S-box search [SA08] for as many parameters as possible. Consequently, the actual number of active S-boxes from the obtained bounds completely corresponded to the results from the exhaustive search with the following parameters: $\mathrm{GFN}_4^{\mathrm{std}}$ with $m = 2, 3, ..., 8$,[4] $\mathrm{GFN}_6^{\mathrm{std}}$ with $m = 2, 3, 4$, $\mathrm{GFN}_8^{\mathrm{std}}$ with $m = 2$, $\mathrm{GFN}_6^{\mathrm{imp}}$ with $m = 2, 3, 4$, and $\mathrm{GFN}_8^{\mathrm{imp}}$ with $m = 2$ and $r = 1$ up to 20, where $\mathcal{B}^D = m + 1$. While we have not confirmed the tightness of the other bounds due to com-

[4]The case of $\mathrm{GFN}_4^{\mathrm{std}}$ with $m = 4$ is in Table 4 of [SA08].

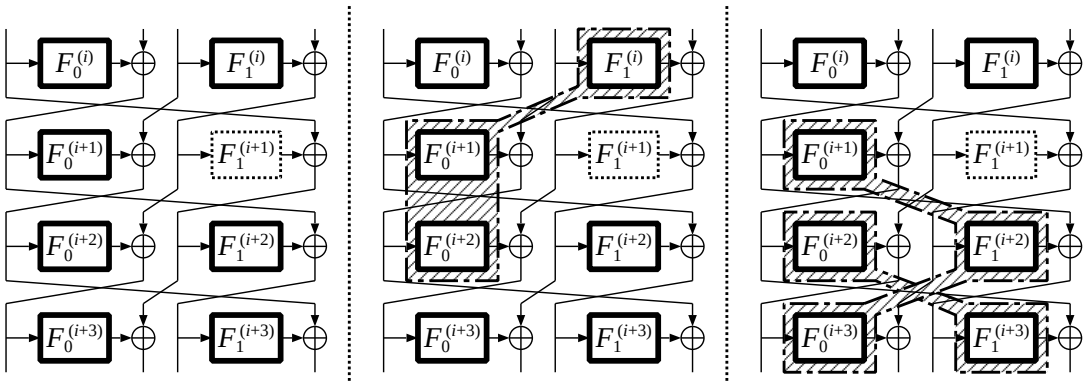

Figure 4.13: An example path of $\mathrm{GFN}_4^{\mathrm{std}}$

putational restrictions of the weight-based exhaustive search, it seems that the obtained bounds are tight as well.

4.5 Linear Active S-Boxes in GFN

It was shown by Kanda [Kan00] that the lower bounds on the minimum number of linear active S-boxes of Feistel structure with SP-type F-functions can be obtained by simply replacing differential branch number $\mathcal{B}^D$ by linear branch number $\mathcal{B}^L$. In his work, Feistel structures with SP-type F-functions can be represented as Feistel structures with PS-type F-functions by using an equivalent transformation. Then the minimum number of active S-boxes is derived by evaluating the transformed cipher using the concatenation rules [Bih94, Mat94].

GFN with SP-type F-functions can be represented as GFN with PS-type F-functions in a similar way. Note that, in contrast to Feistel structures, depending on the original round permutation used in GFN, the transformed round permutation can be different. However, we can use the same algorithm to determine the lower bounds on the minimum number of linear active S-boxes by replacing the original round permutation by the transformed round permutation. This is not the case for the structures in the tables shown in this chapter: the transformed round permutation is the same as the original round permutation. Thus, the minimum number of linear active S-boxes is obtained by simply replacing differential branch numbers $\mathcal{B}^D$ by linear branch numbers $\mathcal{B}^L$.

4.6 Discussion

In this section, we discuss the obtained results. We first give an example of the parameter $m = 4$ and $n = 8$ of $\mathrm{GFN}_8^{\mathrm{std}}$, i.e., 256-bit block cipher, to show applicability of our results. We assume that this example cipher consists of the MDS matrices and the inversion S-boxes over $\mathrm{GF}(2^8)$, specifically, $\mathcal{B}^D = \mathcal{B}^L = 5$ and the maximum differential and linear probability of the S-box is 2^{-6}. In this case, at least 22 active S-boxes are required to be secure against differential and linear attacks, as $(2^{-6})^{22} = 2^{-132} < 2^{-128}$ when the key size is 128-bit. Though the previous result shows that 24 rounds are required to have more

than 22 active S-boxes, our results show that only 10 rounds are required to be secure against differential and linear attacks. Thus, our results are useful to design an efficient symmetric primitive, since the required number of rounds with respect to differential and linear cryptanalysis is reduced. While many types of attacks must be considered when constructing a secure symmetric primitive, actually, differential, linear, impossible differential and saturation attacks tend to be the bottleneck in GFN. Therefore, it can be said that at least two of them can be improved by using the new bounds. If the parameters (the dimension of the matrices m and the partitioning number d) are larger, the effects of our results become even more noticeable.

Moreover, according to our results, most of the bounds on a sufficiently large number of rounds can be derived from bounds on a smaller number of rounds. For example, most of rounds of the minimum number of active S-boxes for more than seven rounds of $\mathrm{GFN}_4^{\mathrm{std}}$ can be derived from the bounds on one to the bounds on six consecutive rounds, e.g. the minimum number of active S-boxes in ten rounds of $\mathrm{GFN}_4^{\mathrm{std}}$ can be represented as active S-boxes in four rounds and six rounds of $\mathrm{GFN}_4^{\mathrm{std}}$. Thus it seems that determining tight bounds for a small number of rounds is important. Therefore, our algorithm works well even if the number of rounds is large, whereas it needs a lot of computation to derive bounds of GFN with large number of rounds, e.g., more than 30 rounds.

Furthermore, the results show that the number of active S-boxes increases about 1.5 times when the partitioning number is doubled, assuming the number of S-boxes used in each F-function remains the same and the number of rounds is sufficiently large.

4.7 Conclusions

In this chapter, we have shown the first tight bounds on the minimum number of active S-boxes of GFN with large parameter sets. We first proved tight lower bounds for four and six rounds of the standard GFN manually. Then, we introduced a novel approach to evaluate the minimum number of active S-boxes of GFN by using the branch number of the matrices used in the structure. The proposed algorithm uses three-round relations of the Feistel connection and well known truncated differential search. By using our algorithm, all types of the GFN can be evaluated precisely, including recently proposed GFN that utilize optimal round permutations instead of the word-based rotation used in the standard GFN. Moreover, we confirmed the tightness of the obtained bounds by comparing with the results obtained by the weight-based exhaustive active S-box search algorithm.

By applying our results, the required number of rounds to be secure against differential and linear attacks can be reduced significantly. Moreover, all bounds obtained in this chapter depend only on the branch number of the matrices used in GFN. The results can therefore be widely used to design an efficient symmetric primitive. In other words, our results are useful not only for more thoroughly understanding the security of the GFN, but also for designing an efficient symmetric key primitive, because the GFN can be implemented compactly and evaluating its security against differential attacks is essential to both block cipher and hash function design.

Table 4.2: The minimum number of active S-boxes in $\mathrm{GFN}_d^{\mathrm{std}}$, assuming $\mathcal{B} > 2$, where $\mathcal{B}$ denotes either the differential or the linear branch number of the matrices used in the GFN

r	BFN	$\mathrm{GFN}_4^{\mathrm{std}}$	$\mathrm{GFN}_6^{\mathrm{std}}$	$\mathrm{GFN}_8^{\mathrm{std}}$	$\mathrm{GFN}_{10}^{\mathrm{std}}$	$\mathrm{GFN}_{12}^{\mathrm{std}}$	$\mathrm{GFN}_{14}^{\mathrm{std}}$	$\mathrm{GFN}_{16}^{\mathrm{std}}$
1	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2
4	$\mathcal{B}$	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$
5	$\mathcal{B}+1$	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$
6	$\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$
7	$\mathcal{B}+3$	$2\mathcal{B}+2$	$2\mathcal{B}+4$	$2\mathcal{B}+4$	$2\mathcal{B}+4$	$2\mathcal{B}+4$	$2\mathcal{B}+4$	$2\mathcal{B}+4$
8	$2\mathcal{B}+1$	$2\mathcal{B}+3$	$3\mathcal{B}+3$	$3\mathcal{B}+3$	$3\mathcal{B}+3$	$3\mathcal{B}+3$	$3\mathcal{B}+3$	$3\mathcal{B}+3$
9	$2\mathcal{B}+2$	$2\mathcal{B}+4$	$3\mathcal{B}+6$	$3\mathcal{B}+6$	$3\mathcal{B}+6$	$3\mathcal{B}+6$	$3\mathcal{B}+6$	$3\mathcal{B}+6$
10	$2\mathcal{B}+3$	$3\mathcal{B}+3$	$4\mathcal{B}+5$	$4\mathcal{B}+5$	$4\mathcal{B}+5$	$4\mathcal{B}+5$	$4\mathcal{B}+5$	$4\mathcal{B}+5$
11	$2\mathcal{B}+4$	$3\mathcal{B}+5$	$4\mathcal{B}+7$	$4\mathcal{B}+8$	$4\mathcal{B}+8$	$4\mathcal{B}+8$	$4\mathcal{B}+8$	$4\mathcal{B}+8$
12	$3\mathcal{B}+2$	$4\mathcal{B}+4$	$5\mathcal{B}+5$	$6\mathcal{B}+6$	$6\mathcal{B}+6$	$6\mathcal{B}+6$	$6\mathcal{B}+6$	$6\mathcal{B}+6$
13	$3\mathcal{B}+3$	$4\mathcal{B}+4$	$5\mathcal{B}+6$	$6\mathcal{B}+6$	$6\mathcal{B}+9$	$6\mathcal{B}+9$	$6\mathcal{B}+9$	$6\mathcal{B}+9$
14	$3\mathcal{B}+4$	$4\mathcal{B}+5$	$6\mathcal{B}+5$	$6\mathcal{B}+7$	$7\mathcal{B}+8$	$7\mathcal{B}+8$	$7\mathcal{B}+8$	$7\mathcal{B}+8$
15	$3\mathcal{B}+5$	$4\mathcal{B}+6$	$6\mathcal{B}+7$	$6\mathcal{B}+8$	$7\mathcal{B}+12$	$7\mathcal{B}+12$	$7\mathcal{B}+12$	$7\mathcal{B}+12$
16	$4\mathcal{B}+3$	$5\mathcal{B}+5$	$7\mathcal{B}+6$	$7\mathcal{B}+7$	$9\mathcal{B}+9$	$9\mathcal{B}+9$	$9\mathcal{B}+9$	$9\mathcal{B}+9$
17	$4\mathcal{B}+4$	$5\mathcal{B}+7$	$7\mathcal{B}+8$	$7\mathcal{B}+9$	$9\mathcal{B}+13$	$9\mathcal{B}+13$	$9\mathcal{B}+13$	$9\mathcal{B}+13$
18	$4\mathcal{B}+5$	$6\mathcal{B}+6$	$8\mathcal{B}+7$	$8\mathcal{B}+8$	$10\mathcal{B}+8$	$10\mathcal{B}+12$	$10\mathcal{B}+12$	$10\mathcal{B}+12$

Table 4.3: The minimum number of active S-boxes in $\mathrm{GFN}_d^{\mathrm{imp}}$, assuming $\mathcal{B} > 2$, where $\mathcal{B}$ denotes either the differential or the linear branch number of the matrices used in the GFN

rounds	$\mathrm{GFN}_6^{\mathrm{imp}}$	$\mathrm{GFN}_8^{\mathrm{imp}}$	$\mathrm{GFN}_{10}^{\mathrm{imp}}$	$\mathrm{GFN}_{12}^{\mathrm{imp}}$	$\mathrm{GFN}_{14}^{\mathrm{imp}}$	$\mathrm{GFN}_{16}^{\mathrm{imp}}$
1	0	0	0	0	0	0
2	1	1	1	1	1	1
3	2	2	2	2	2	2
4	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$	$\mathcal{B}+1$
5	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$	$\mathcal{B}+3$
6	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$	$2\mathcal{B}+2$
7	$2\mathcal{B}+4$	$2\mathcal{B}+4$	$2\mathcal{B}+4$	$2\mathcal{B}+4$	$2\mathcal{B}+4$	$2\mathcal{B}+4$
8	$4\mathcal{B}+2$	$4\mathcal{B}+3$	$4\mathcal{B}+3$	$3\mathcal{B}+3$	$4\mathcal{B}+3$	$4\mathcal{B}+3$
9	$4\mathcal{B}+4$	$4\mathcal{B}+6$	$5\mathcal{B}+4$	$3\mathcal{B}+6$	$5\mathcal{B}+4$	$5\mathcal{B}+6$
10	$4\mathcal{B}+6$	$5\mathcal{B}+4$	$6\mathcal{B}+4$	$5\mathcal{B}+4$	$7\mathcal{B}+2$	$7\mathcal{B}+5$
11	$4\mathcal{B}+8$	$5\mathcal{B}+7$	$6\mathcal{B}+6$	$5\mathcal{B}+7$	$7\mathcal{B}+5$	$8\mathcal{B}+8$
12	$6\mathcal{B}+2$	$7\mathcal{B}+4$	$7\mathcal{B}+10$	$7\mathcal{B}+4$	$9\mathcal{B}+4$	$10\mathcal{B}+4$
13	$6\mathcal{B}+3$	$7\mathcal{B}+5$	$8\mathcal{B}+4$	$8\mathcal{B}+5$	$10\mathcal{B}+4$	$11\mathcal{B}+5$
14	$6\mathcal{B}+8$	$8\mathcal{B}+4$	$9\mathcal{B}+3$	$9\mathcal{B}+8$	$11\mathcal{B}+5$	$12\mathcal{B}+3$
15	$6\mathcal{B}+10$	$8\mathcal{B}+6$	$9\mathcal{B}+5$	$9\mathcal{B}+12$	$11\mathcal{B}+8$	$12\mathcal{B}+10$
16	$8\mathcal{B}+6$	$9\mathcal{B}+5$	$10\mathcal{B}+4$	$10\mathcal{B}+10$	$13\mathcal{B}+6$	$15\mathcal{B}+1$
17	$8\mathcal{B}+8$	$9\mathcal{B}+7$	$10\mathcal{B}+6$	$10\mathcal{B}+14$	$14\mathcal{B}+6$	$15\mathcal{B}+3$
18	$8\mathcal{B}+10$	$10\mathcal{B}+6$	$12\mathcal{B}+5$	$12\mathcal{B}+8$	$16\mathcal{B}+3$	$17\mathcal{B}+2$

Chapter 5

Efficient Design of 3-Line Generalized Feistel Networks

5.1 Introduction

5.1.1 GFN with 3 Lines and Double SP-Functions

The problem of differential and linear cryptanalysis has not been addressed so far for 3-line GFNs (GFN_3) with double SP-functions and single-round diffusion. At the same time, it is exactly the combination of 3 lines and double SP-functions that appears most promising for GFNs with more than 2 lines: there is evidence that both going from 4 lines to 3 lines in Feistel networks [Bog11] and from single SP-functions to double SP-functions [BS13] as indicated above tend to increase efficiency with respect to differential and linear cryptanalysis. For comparing efficiency, the works [Bog11] and [BS13] as well as this chapter use the proportion of active S-boxes in all S-boxes – a valid efficiency metric introduced in [SP04] for ciphers based on substitution-diffusion transforms.

Figure 5.1 depicts GFN_3 we will be studying in this chapter. This GFN structure is the only (up to equivalence) non-contracting 3-line GFN, when the definition of a GFN implies that the lines are only updated by XOR with the output of a round function, the lines are rotated by one position between rounds, and a line cannot be both source and destination within one round. All other GFNs with 3 lines under this definition will be contracting and, thus, manifest a strong differential effect similar to that discussed in [Bog11].

The double SP-function is also demonstrated in Fig. 5.1: it consists of two SP-maps, each comprising a key addition layer (subkeys $k_i^{(u)}$), an S-box layer (with m S-boxes s_j), and a diffusion matrix M. The second linear layer limits the differential effect that might be present for SPS-functions.

5.1.2 Contributions

In this chapter, we prove that every 7 rounds of such GFN_3 with double invertible SP-functions add at least $4\mathcal{B}$ active S-boxes, both differentially and linearly, where $\mathcal{B}$ is the branch number of the diffusion matrix M (or its transpose) used in the round functions (Section 5.2). Conforming to the intuition outlined above, this indeed guarantees a

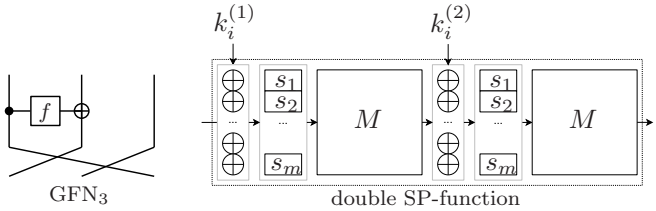

Figure 5.1: GFN$_3$ and double SP-function

proportion of active S-boxes by up to 14% higher than that for GFN$_4$-I and GFN$_4$-II with double SP-functions (Section 5.3), when instantiated with MDS matrices.

5.2 Minimum Number of Active S-Boxes for GFN$_3$

In this section, we prove a lower bound on the number of differentially and linearly active functions for GFN$_3$ with invertible functions, transform it to a lower bound on the number of differentially and linearly active S-boxes, and demonstrate the tightness of these bounds. We perform our proof for differential cryptanalysis and show how it literally translates to linear cryptanalysis. In the proof, we start with the local constraints on the truncated trails of GFN$_3$, introduced in Fig. 5.2, and then show how those lead to properties over 7 rounds. In Fig. 5.2, $\delta_{i+j}, \gamma_{i+j} \in \{0, 1\}$, where $\delta_{i+j} = 1$ or $\gamma_{i+j} = 1$ indicate that the line is differentially or linearly active, respectively.

5.2.1 Constraints on Truncated Differential Trails

Consider the XOR update of line i: it connects the truncated differences of lines i, $i+2$ and $i+3$. As the function is invertible, its output difference cannot be zero for a non-zero input difference. Then due to the properties of the XOR, one has:

Rule 1 (Differential zero rule for GFN$_3$). *For any i, if two of δ_i, δ_{i+2}, δ_{i+3} are zero, then all of them are zero. This is called an all-zero XOR.*

Rule 2 (Differential non-zero rule for GFN$_3$). *For any i, if δ_i, δ_{i+2}, δ_{i+3} are not all zero, at least two of them are non-zero. This is called an non-zero XOR.*

Rule 2 is restrictive enough to yield

Proposition 1 (Relation between active lines and non-zero XORs). *For GFN$_3$ with invertible functions, the number of active lines over t consecutive functions is greater or equal to the number of non-zero XORs over t consecutive functions plus one, given a non-trivial input difference.*

Proof. Since any two sets of lines connecting to two non-zero XORs have at most one overlapping line from Rule 2, the number of active lines is bounded by the number of non-zero XORs. □

In the sequel, we will use the constraints discussed above to derive limitations for truncated trails over 7 rounds of GFN$_3$.

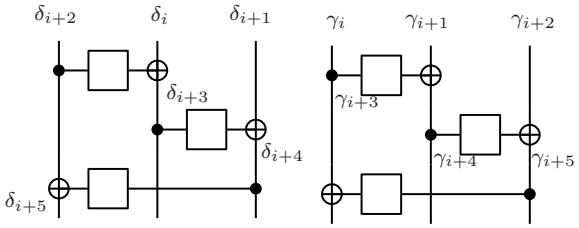

Figure 5.2: Truncated differential and linear trails (3 rounds) for 3-line GFN

5.2.2 Differentially Active Functions

Lemma 1. *For GFN_3 with invertible functions, every non-trivial differential trail over 7 rounds with at most one all-zero XOR has at least 4 active functions.*

Proof. Since at least $7 - 1 = 6$ XORs over 7 rounds are non-zero, there exist at least 7 active lines from Proposition 1. Up to 3 of active lines are not counted, since the corresponding differences do not enter any functions within the 7 rounds. This gives at least $7 - 3 = 4$ non-zero active lines and at least 4 active functions. □

Lemma 2. *For GFN_3 with invertible functions, every non-trivial differential trail over 7 rounds without consecutive all-zero XORs has at most one all-zero XOR.*

Proof. From Rules 1 and 2, the following truncated differential trail is derived with no consecutive all-zero XORs: if the XOR of function i of GFN_3 is all-zero and there are no consecutive all-zero XORs, the forward and backward difference propagations will follow the truncated differential trail:

$$\delta_{i-3}\delta_{i-2}\delta_{i-1}\delta_i\delta_{i+1}\delta_{i+2}\delta_{i+3}\delta_{i+4}\delta_{i+5}\delta_{i+6} = 1110100111. \tag{5.1}$$

From this trail, the first possible all-zero XOR appears in function $i + 7$ in the forward difference propagation. Similarly, in the backward direction, the first possible all-zero XOR appears in function $i - 7$. Thus, there exists at most one all-zero XOR over 7 rounds, since there are at least six consecutive non-zero XORs after and before an all-zero XOR. □

Lemma 3. *For GFN_3 with invertible functions, no non-trivial differential trail can have any consecutive all-zero XORs.*

Proof. Suppose that the XORs of both functions i and $i + 1$ are all-zero. In that case, δ_i, δ_{i+2} and δ_{i+3} are all zero due to Rule 1. Also, δ_{i+1} and δ_{i+4} are both zero. For any i, δ_i, δ_{i+1} and δ_{i+2} cannot be zero simultaneously due to invertibility. Thus, the XORs of functions i and $i + 1$ cannot be all-zero simultaneously, then we obtain that there does not exist consecutive all-zero XOR in GFN_3. □

Directly combining Lemmata 1 to 3, one obtains

Proposition 2 (Differentially active functions for $\mathbf{GFN}_3$). *GFN_3 with invertible functions provides at least 4 differentially active functions over 7 consecutive rounds for each non-trivial input difference.*

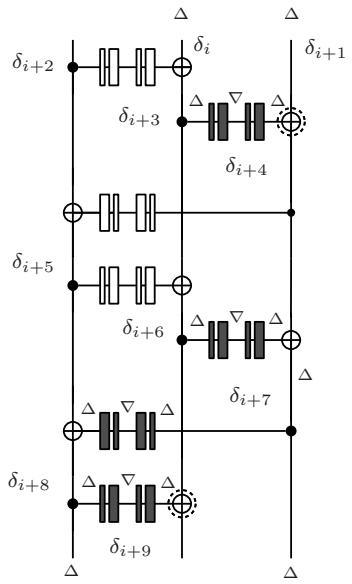

Figure 5.3: Truncated differential trail of GFN_3 with double SP-functions (7 rounds) attaining the lower bounds of Theorem 3 for MDS matrices

5.2.3 Linearly Active Functions

For GFN_3, the constraints of Rules 1 and 2 as well as the statements Proposition 1 and Lemmata 1 to 3 with respect to truncated *differential* trails literally translate to those with respect to truncated *linear* trails: truncated differential trail $\delta_i \dots \delta_{i+t-1}$ of length t corresponds to truncated linear trail $\gamma_i \dots \gamma_{i+t-1}$ under the change of variables $\delta_{i+j} \mapsto \gamma_{i+t-1-j}$, $j \in \{0, \dots, t-1\}$. Thus, one does not have to repeat the reasonings and can directly obtain the linear version of the differential Proposition 2:

Proposition 3 (**Linearly active functions for GFN_3**). *GFN_3 with invertible functions provides at least 4 linearly active functions over 7 consecutive rounds for any non-trivial input/output linear mask values.*

5.2.4 Active S-Boxes and Tightness of Bounds

Due to the presence of the second S-box layer, whenever a double SP-function is active either differentially or linearly, it provides at least $\mathcal{B}$ active S-boxes, where $\mathcal{B}$ is the *branch number* [DR02] of the underlying diffusion matrix M or its transpose. Thus, from Propositions 2 and 3, one can straightforwardly derive

Theorem 3 (**Active S-boxes for GFN_3**). *Every $7R$, $R \geq 1$, rounds of the 3-line GFN with invertible double SP-functions provide at least $4\mathcal{B}R$ active S-boxes (differentially or linearly), where $\mathcal{B}$ is the branch number of the diffusion matrix in the SP-functions or its transpose.*

The lower bounds of Theorem 3 on the number of active S-boxes are actually tight, since there exist S-box truncated trails attaining those minimal numbers. In Fig. 5.3, we

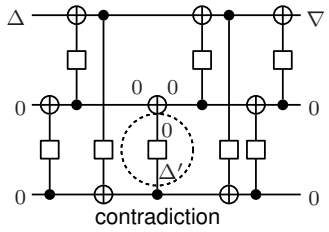

Figure 5.4: 8-round impossible differential for GFN_3 with bijective functions for non-zero Δ, Δ', and ∇

demonstrate a 7-round differential trail for GFN_3 with double SP-functions and MDS diffusion having $4(m+1)$ active S-boxes, where Δ and ∇ denote S-box truncated differences with only one S-box active out of m (Δ) and all m S-boxes active (∇), respectively. In Fig. 5.3, the trail is iterative and corresponds to (5.1) from δ_i to δ_{i+6}, XORs with difference cancellation are marked with dashed circles, and differentially active functions are denoted by grey shading. MDS matrices are diffusion-optimal with their branch numbers being maximum possible and equal to $\mathcal{B}(M) = m + 1$ [DR02, LN97].

Note that the input and output differences for each of the functions active in the trails contain exactly one active component. At the same time the internal difference in each of them involves all S-boxes. This 7-round trail for GFN_3 is iterative and illustrates the tightness of Theorem 3 for any R.

5.2.5 Resistance to Other Attacks

There are several analysis approaches to be considered other than differential and linear cryptanalysis in order to design a secure block cipher.

Most Feistel structures with invertible functions have relatively long impossible differentials due to their comparatively slow diffusion. For instance, 5-round, 19-round, and 9-round impossible differentials exist for balanced Feistel, GFN_4-I, and GFN_4-II, respectively [CY09, TTS$^+$08]. We notice that impossible differential cryptanalysis [BBS99, BKR97] can also be applicable to GFN_3. The longest impossible differential we found for GFN_3 is over 8 rounds of the form $(0, 0, \Delta) \nrightarrow (\nabla, 0, 0)$ for any non-zero Δ and ∇ as illustrated in Fig. 5.4.

Cancellation cryptanalysis [BDLF10] is an attack technique for GFN-type hash functions also applicable to the block cipher underlying the Lesamnta hash function [HKY00] which is based on type-I GFN structure. However, the attack complexity heavily depends on the underlying key schedule and the amount of key input into each function. Thus the cancellation cryptanalysis becomes less efficient for GFN_3 with double SP-functions, since several subkeys are inserted in each function. Three-subset meet-in-the-middle cryptanalysis [BR10] is a recent attack on block ciphers having a simple key schedule and slow diffusion. However, for GFN_3, the attack is likely to be thwarted by a reasonable key schedule over a non-negligible number of rounds.

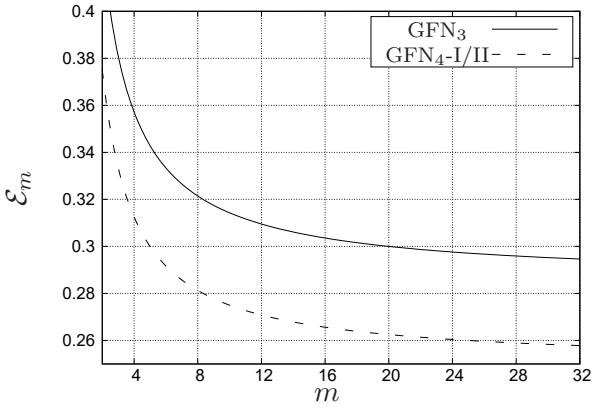

Figure 5.5: Advantage of GFN_3 over GFN_4-I/II with double SP-functions: efficiency $\mathcal{E}_m$, where each S-layer has m S-boxes

5.3 Differential and Linear Efficiency

In this section, we compare the efficiency of GFN_3 based on the results of this chapter to that of GFN_4-I and GFN_4-II with double SP-functions of [BS13]. Note that for GFN_4 double SP-functions provide an efficiency advantage of up to 50% over single SP-functions. The comparison in this section is performed for MDS matrices.

We use the efficiency metrics $\mathcal{E}_m$ and $\mathcal{E}$ defined in Section 3.2. Note that the asymptotic treatment of efficiency is purely technical and does not impose any constraints in practice, if the bounds on $\mathcal{NA}_{m,r}$ are tight and the corresponding trails are iterative, which is the case for both GFN_3 and GFN_4 under consideration.

As discussed in Section 3.2.2, the metrics $\mathcal{E}_m$ and $\mathcal{E}$ do not take into account the costs of the linear diffusion, whose matrix will be slightly larger for 3-line GFNs. However, with respect to the time performance of software implementations on modern 32- and 64-bit processors – a major application platform – the cost of the matrix-vector multiplications can be ignored, since most implementations combine the latter with S-box invocations in the same table lookup, the overhead being negligible for most practical block sizes.

Using Theorem 3 for GFN_3 and the corresponding results for GFN_4 from [BS13], stating that every 14 rounds of GFN_4-I and every 6 rounds of GFN_4-II add $7\mathcal{B}$ and $6\mathcal{B}$ active S-boxes, respectively, one obtains:

$\mathcal{E}_m = \frac{4(m+1)}{7(2m)} = \frac{2m+2}{7m}$ for GFN_3 and $\mathcal{E}_m = \frac{7(m+1)}{14(2m)} = \frac{6(m+1)}{6(4m)} = \frac{m+1}{4m}$ for GFN_4-I/II,
$\mathcal{E} = \frac{2}{7} \approx 0.286$ for GFN_3 and $\mathcal{E} = \frac{1}{4} = 0.25$ for GFN_4-I/II

with double SP and MDS diffusion.

Figure 5.5 provides a comparison between these two efficiencies for a relevant range of m's. When instantiated with double SP-functions, GFN_3 tends to be consistently more efficient (with respect to differential and linear cryptanalysis) than GFN_4-I/II, the advantage growing with the block size and attaining its maximum of about 14% for long blocks (like in wide-block encryption or hash functions).

These results as well as a relatively low number of rounds covered by the longest known impossible differential suggest that 3-line GFNs with double SP-functions are

likely to yield more efficient ciphers in practice than 4-line GFNs with single and double SP-functions.

5.4 Conclusions

In this chapter, we investigated the design of F-functions utilized in 3-line GFNs. We proposed to instantiate the GFNs with double SP-functions instead of single SP-functions. Then we proved tight lower bounds on the number of active S-boxes for the proposed constructions. Moreover, it was shown that the proportion of active S-boxes in all S-boxes for 3-line GFNs with double SP-functions is by up to 14% higher than that for type-I and type-II 4-line GFNs with double SP-functions, when instantiated with MDS matrices. While the block size of a cipher consisting of 3-line GFNs cannot be well used one such as 64-bit or 128-bit, our results imply the possibility of designing more efficient block cipher with $3m$-block size, e.g., 48-bit or 96-bit, which are known as suitable for RFID tags, where m is a positive integer.

Chapter 6

Classification and Efficient Design of 4-Line Generalized Feistel Networks

6.1 Introduction

In this chapter, we classify 4-line GFNs and propose to instantiate type-I and type-II GFNs with SPS-functions (two substitution layers separated by a permutation layer) or double SP-functions (two subsequent substitution-permutation layers) and single-round diffusion (i.e. using the same diffusion matrix in all diffusion layers of the cipher). We obtain tight lower bounds on the number of active S-boxes in such constructions and demonstrate that this instantiation is more efficient with respect to differential and linear cryptanalysis than using single SP-functions for this purpose in terms of the proportion of active S-boxes.

6.1.1 Related Work

For BFNs, the work [Kan00] proves the minimum number of active S-boxes in BFNs with SP-functions when the diffusion matrix is the same in all rounds (*single-round diffusion*). The papers [SS04, SS06] deal with the difference cancellation effect for such BFNs and introduces the diffusion switching mechanism which relies on using several distinct diffusion matrices over multiple rounds (*multiple-round diffusion*). The lower bounds on the number of active S-boxes for BFN with SP-functions and multiple-round diffusion are proven in [SP04]. Those for BFNs with SPS-functions and single-round diffusion are analyzed in [Bog10]. Note that using distinct diffusion matrices in different rounds (as required by the multiple-round diffusion) reduces the efficiency of an implementation.

For GFNs, lower bounds on the number of active S-boxes are obtained for type-I and type-II GFNs with SP-functions and single-round diffusion in [WZL06] and [Shi10], respectively. Bounds for unbalanced Feistel networks with contracting multiple-round diffusion are derived in [Bog11]. Rough lower bounds for type-I and type-II with single SP-functions and multiple-round diffusion were proven by [SA08]. The work [SA08] also provides some numeric analysis for two specific cases of type-I and type-II GFNs with single SP-functions and multiple-round diffusion.

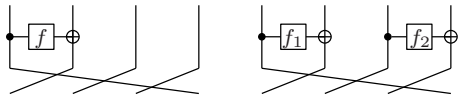

Figure 6.1: Round transforms of type-I and type-II GFNs with 4 lines

6.1.2 Contributions and Outline

Definition and classification of GFNs with 4 lines.

Despite the wide use of GFNs, it is not clear what the exact definition of a GFN is. In the broad sense, any type of invertibly combining several keyed nonlinear functions using XOR operations and permutations can be called a GFN. In a slightly narrower sense, such a combination of functions can be considered a GFN only when the rounds are connected by a rotation by one line instead of a generic line permutation. Further restrictions can be imposed by a definition such as the usage of not necessarily invertible round functions (which excludes Skipjack-like constructions).

In this chapter, we propose a definition of a GFN which is based on three main restrictions. First, a line can be only updated by XORing the output of a function (and not e.g. by applying the function itself to the line). Second, in a single round, a line cannot be source and destination at the same time. Third, rounds are connected by the rotation of lines by one position. See Section 6.2.

Under this definition, we exhaustively enumerate all 4-line GFNs up to cyclic equivalence. It turns out that there are 21 constructions up to the equivalence. As we are mostly interested in differential and linear properties of GFNs, we notice that most of these constructions lose significant parts of their differential security, since multiple differential trails contribute to the same differential. We call GFNs with this property *contracting* (that is, when the same line is updated more than once before it is used as an input to a function). We find that there are exactly 4 non-contracting GFNs with 4 lines under our definition. Namely, type-I and type-II GFNs in the terminology of [ZMI89b] which are illustrated in Fig. 6.1 and their inverses up to permutational equivalence. All the other 4-line GFNs exhibit a differential effect, since at least one line is XOR-updated more than once before being used as an input to a function there [Bog11]. This effectively reduces the proportion of active S-boxes for contracting GFNs, which is not the case for type-I and type-II GFNs. Moreover, we exhaustively search the minimum numbers of active functions for contracting GFNs up to 50 rounds. The numeric search results show that only 2 contracting GFNs have slightly more active functions compared to type-I and type-II GFNs, and the other contracting GFNs have less active functions. This implies that the contracting GFNs do not have advantages with respect to differential security due to a strong differential effect and almost same number of active functions compared to non-contracting GFNs.

GFNs with SPS-functions or double SP-functions.

We propose to instantiate the type-I and type-II GFNs with invertible SPS-functions (two substitution layers separated by a permutation layer) or double SP-functions (substitution-

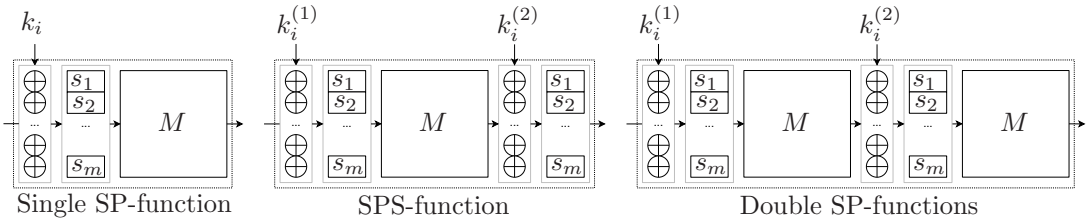

Figure 6.2: Single SP-function, SPS-function and double SP-functions

permutation layer followed by another substitution-permutation layer) instead of single SP-functions (one substitution-permutation layer), see Fig. 6.2. The intuition behind this specific choice of functions is as follows:

- Due to the second S-box layer, SPS-functions or double SP-functions allow, on the one hand, to limit the analysis to the differential and linear activity patterns of functions and, on the other hand, to have effectively a higher number of active S-boxes.
- Compared with an instantiation with double SP-functions (substitution-permutation layer followed by another substitution-permutation layer), that with SPS-functions has the same number of active S-boxes. However, the double SP construction has two times larger number of permutation layers than the SPS construction, which may reduce the efficiency.
- The second diffusion layer of a double SP-function constrains the differential effect (many differential trails contributing to the same differential) which might be present for SPS-functions.
- Having an odd number of SP-layers does not enable to prove tight bounds on the number of active S-boxes by working with functions. An even number of SP-layers is similar to the case of double SP-functions. We also conjecture that functions with more than 2 SP-layers do not add on the efficiency of the construction, thus, double SP-functions providing a better efficiency.
- The invertibility prevents a function from absorbing differences: If a nonzero difference enters a bijective function the output difference will also be nonzero.

Truncated trails and proven lower bounds on active functions.

We use a string-based technique to prove tight lower bounds on the number of differentially and linearly active functions for the GFNs. We demonstrate an equivalence between truncated differential and linear trails as well as imposed structural constraints which allows to work with both differential and linear cryptanalysis simultaneously (Section 6.3).

We prove that, for 4-line type-I and type-II GFNs with invertible functions, at least a half of their functions over 14 and 6 rounds, respectively, are active (Section 6.4). Note that this is not necessarily the case for GFNs with more than 4 lines: type-II GFNs with 8 lines do not seem to provide a proportion of more than 0.35 active functions [SM10].

Apart from our constructions with SPS-functions, this result also directly applies to the block cipher E^{512} underlying the compression function C^{512} of the second-round SHA-3 candidate SHAvite-3_{512} [DB09] and improves the upper bound on the differential trail probability over 9 rounds from 2^{-678} down to 2^{-904}.

Improved efficiency of GFNs.

For SPS-functions or double SP-functions, the lower bound on the number of active functions for type-I and type-II GFNs directly translates to the lower bound on the number of active S-boxes. Based on the proven bounds, we show that the instantiation with SPS-functions or double SP-functions provides a proportion of differentially and linearly active S-boxes by up to 33% and 50% higher than that with single SP-functions using MDS diffusion for type-I and type-II GFNs, respectively, if the same diffusion matrix is used in all rounds. In other words, GFNs with SPS-functions or double SP-functions outperform GFNs with single SP-functions in terms of differential and linear efficiency by a considerable margin. This opens up the possibility of designing more efficient block ciphers based on GFN structures (Section 6.5).

Provable security for GFNs against differential and linear attack.

Besides security against differential and linear attacks, further analyses including impossible differential cryptanalysis, zero-correlation linear cryptanalysis and cancellation cryptanalysis for GFNs are discussed. Furthermore, we show the upper bounds on the differential and the linear hull probability of 4-line type-II GFNs with SPS-functions or double SP-functions, which are directly obtained from the results on the provable security for the SPN structure and the type-II GFN (Section 6.6).

6.2 Classification of GFNs with 4 Lines

We give a definition of a GFN with ℓ lines to perform the classification:

Definition 16 (GFN with ℓ lines). *Let the state of a block cipher with a b-bit block size be represented by ℓ equally wide parts, called lines, of b/ℓ bits each, $\ell | b$. This block cipher is called a generalized Feistel network with ℓ lines if its round transformation can be presented by operations on the ℓ lines with the following restrictions:*

1. *The lines are rotated by one position to the left between the rounds.*
2. *Each line is used in exactly one of the following three ways:*
   - *It is source of a keyed domain-preserving nonlinear function acting on b/ℓ bits.*
   - *It is destination of a keyed domain-preserving nonlinear function acting on b/ℓ bits. The line is updated by XORing the output of the function to it.*
   - *It is neither source nor destination.*
3. *The structure attains full diffusion after a finite number of rounds.*

Restriction 1 in Definition 16 of rotating the lines between the rounds originates from the fact that we are mostly interested in 4-line GFNs. The work [SM10] studies the diffusion properties of type-II GFNs when another type of line permutation between rounds is allowed to be chosen. The results of [SM10] suggest that line permutations other than rotations by one position may indeed result in faster diffusion and more security against impossible differential attacks when the number of lines is 6 and more. However, the results show that there is no gain at least with respect to diffusion when the number of lines is 4, since there are only three variations of line permutations which are right and left rotations, and Nyberg's GFN [Nyb96]. That is why the consideration of [SM10] is limited to 6 lines and more. That is, GFNs with just 4 lines are unlikely to benefit from other types of line permutation.

A specific GFN under Definition 16 will be characterized by connections between the lines within one round. Some types of connections will result in similar or even equivalent GFNs. Let GFN_1 and GFN_2 be two GFNs given by their respective line connections under Definition 16. In the classification, we rely on the following two notions of equivalence between GFNs:

Definition 17 (**Cyclic equivalence**). *GFN_1 and GFN_2 are cyclically equivalent if the line connections within one round of GFN_1 can be obtained from the line connections within one round of GFN_2 by a cyclic rotation of lines.*

Definition 18 (**Permutational equivalence**). *GFN_1 and GFN_2 are permutationally equivalent if, for some positive integer r and any positive integer t, the line connections of every $t \cdot r$ consecutive rounds of GFN_1 can be obtained from the line connections of some $t \cdot r$ consecutive rounds of GFN_2 by permuting input and output lines only.*

We find that there are 21 GFNs with 4 lines under Definition 16 up to the cyclic equivalence of Definition 17, shown in Fig. 6.3 grouped according to the number of functions in a round. In Fig. 6.3, for each GFN type, the number of functions required for full diffusion are provided near the left upper corner of the structure. As we are mostly interested in differential and linear properties of GFNs, we notice that most of these constructions lose significant parts of their differential security, since multiple differential trails contribute to the same differential.

This property occurs iff the same line is updated more than once before it is used as an input to a function:

Definition 19 (**Contracting GFNs**). *A GFN under Definition 16 is called contracting, if the same line is updated more than once before it is used as an input to a function.*

A contracting GFN is also considered as source-heavy Feistel structure which consists of round functions with more than one line of input such as RC2 [Riv98] and SHA-2 [Nat02]. However, in this work, we treat only the contracting round function whose outputs are contracted by the XOR. For instance, GFN3.4 in Fig. 6.3 is a source-heavy Feistel structure with a round function having 3 line inputs and 1 line output. The opposite of the contracting property is the expanding property which occurs whenever a line is used as an input to a function more than once before it gets updated:

Definition 20 (**Expanding GFNs**). *A GFN under Definition 16 is called expanding, if a line is used as an input to a function more than once before it gets updated.*

An expanding GFN is also regarded as target-heavy Feistel structure which consists of round functions with more than one line of output such as MARS [BCD+99] and FORK-256 [HCS+06]. For example, GFN3.1 in Fig. 6.3 is a target-heavy Feistel structure with a round function consisting of 1 line input and 3 line outputs. It is easy to see that contracting GFNs are exactly expanding GFNs. This might be not obvious when considering the round transform of a GFN only, however, becoming clear when the GFN transform over several rounds are treated.

Proposition 4 (**Contracting and expanding GFNs**). *Each contracting GFN under Definition 16 is also necessarily expanding and vice versa.*

This means that the unpleasant property of differentials consisting of multiple differential trails also necessarily occurs in expanding GFNs and have to be eliminated to achieve a good level of resistance against differential cryptanalysis in an efficient way. We refer to the work [Bog11] for a comprehensive study of contracting GFNs with SP-type functions. It suggests that contracting GFNs are much more efficient with respect to linear cryptanalysis and can be utilized whenever linear resistance is of primary relevance. At the same time, they cannot provide the full differential resistance which leads to a considerable reduction of differential efficiency. This makes contracting GFNs much less interesting that non-contracting ones. Moreover, we confirm that the minimum number of active functions of most of the contracting and expanding GFNs are actually lower than that of non-contracting GFNs by numerical experiments, while we do not have tight bounds on the number of active functions for those GFNs. This implies that not only the contracting or expanding constructions have a differential effect but the relative number of active functions is lower for it, resulting in a lower efficiency (see Section 6.4.4).

Among the 21 GFNs shown in Fig. 6.3, only 4 are non-contracting (i.e. where a line is updated exactly once before it is used as an input to a function), namely, type-I (GFN1.2) and type-II (GFN2.1) GFNs in the terminology of [ZMI89b] (Fig. 6.1) as well as two their inverses (GFN1.1 also known as type-III [ZMI89b] and GFN2.2) up to the permutational equivalence of Definition 18. Hence, due to the differential effect present in the contracting GFNs at the example of GFN3.4, our attention will be drawn to the latter two types of GFNs with 4 lines in the sequel.

Note that there can exist further equivalence types (beyond cyclic and permutational) which are, however, out of scope here, since we filter out most GFNs due to the differential effect [Bog11] and the two equivalence notions appear to be enough for determining equivalent designs among the remaining GFNs.

6.3 Equivalence of Differential and Linear Truncated Trails

Here we analyze constraints on the truncated differential and linear trails of type-I and type-II GFNs. We demonstrate an equivalence between differential and linear truncated trails for the GFNs with respect to these constraints. This allows to study truncated differential and linear trails simultaneously by treating them as bit strings.

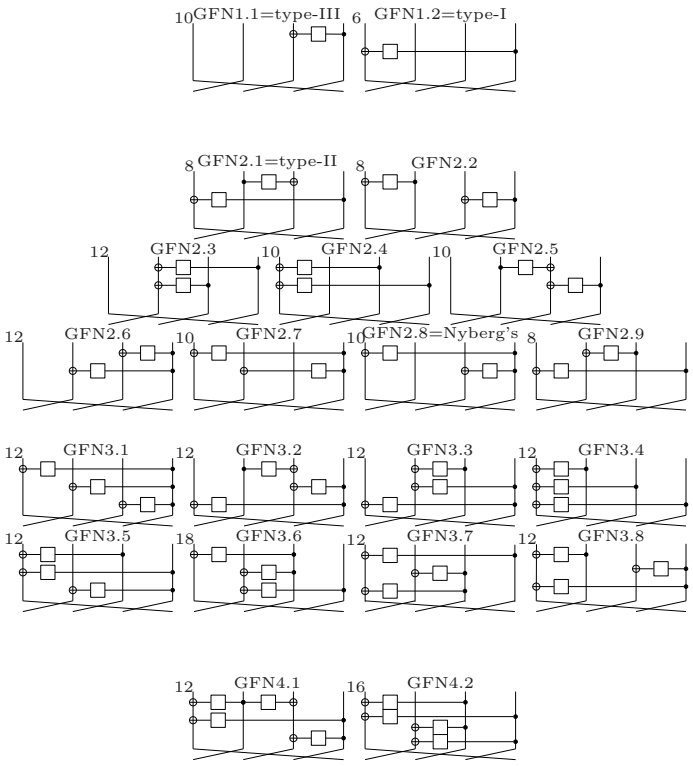

Figure 6.3: Round transforms of the 21 GFNs with 4 lines under Definition 16 distinct up to cyclic equivalence

6.3.1 Truncated Differential Trails and Constraints

A differential trail for an iterative block cipher is a sequence of input and output differences for the consecutive rounds of the cipher. Let

$$\Delta x_i, \Delta x_{i+1}, \Delta x_{i+2}, \Delta x_{i+3}$$

be the input difference to a type-I or type-II GFN with 4 lines. Then a differential trail over t functions is the sequence of $t+4$ differences

$$\Delta x_i, \Delta x_{i+1} \ldots, \Delta x_{i+t+2}, \Delta x_{i+t+3}.$$

Let the bit value δ_{i+j} be defined as:

$$\delta_{i+j} = \begin{cases} 0, & \text{if } \Delta x_{i+j} = 0 \\ 1, & \text{if } \Delta x_{i+j} \neq 0 \end{cases} \quad \text{for } j \in \{0, \ldots, t+3\}.$$

Then the string of $t+4$ bits

$$\delta_i, \delta_{i+1}, \ldots, \delta_{i+t+3} \tag{6.1}$$

is called a *truncated differential trail* over t functions illustrated in Fig. 6.4. In the figure, $\delta_{i+j} \in \{0, 1\}$, where $\delta_{i+j} = 1$ indicates that the line is differentially active.

Due to the properties of XOR used to update lines and the invertibility of the functions, the propagation of differences through type-I and type-II GFNs with 4 lines obeys the following rules:

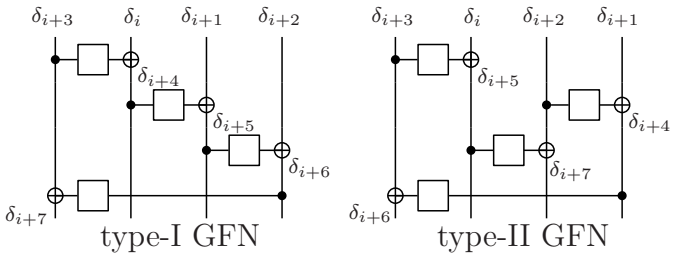

Figure 6.4: Truncated differential trails of type-I (4 rounds) and type-II (2 rounds) GFNs with 4 lines

Property 6 (**Differential zero rule for type-I GFN**). *If two of δ_i, δ_{i+3}, δ_{i+4} are zero, then all of them are zero, where $i = 0, 1, 2, \ldots$*

Property 7 (**Differential nonzero rule for type-I GFN**). *If δ_i, δ_{i+3}, δ_{i+4} are not all zero, at least two of them are nonzero, where $i = 0, 1, 2, \ldots$*

Property 8 (**Differential zero rule for type-II GFN**). *If two of δ_i, δ_{i+3}, δ_{i+5} are zero, then all of them are zero. Similarly, if two of δ_{i+1}, δ_{i+2}, δ_{i+4} are zero, then all of them are zero, where $i = 0, 2, 4, \ldots$*

Property 9 (**Differential nonzero rule for type-II GFN**). *If δ_i, δ_{i+3}, δ_{i+5} are not all zero, at least two of them are nonzero. Similarly, if δ_{i+1}, δ_{i+2}, δ_{i+4} are not all zero, at least two of them are nonzero, where $i = 0, 2, 4, \ldots$.*

6.3.2 Truncated Linear Trails and Constraints

A linear trail for an iterative block cipher is a sequence of input and output selection patterns (also known as linear mask values) for the consecutive rounds of the cipher. Let

$$\Gamma x_i, \Gamma x_{i+1}, \Gamma x_{i+2}, \Gamma x_{i+3}$$

be the input selection pattern for a type-I or type-II GFN with 4 lines. Then a linear trail over t functions is the sequence of $t + 4$ selection patterns

$$\Gamma x_i, \Gamma x_{i+1} \ldots, \Gamma x_{i+t+2}, \Gamma x_{i+t+3}.$$

Similarly to truncated differential trails, let the bit value γ_{i+j} be defined as:

$$\gamma_{i+j} = \begin{cases} 0, & \text{if } \Gamma x_{i+j} = 0 \\ 1, & \text{if } \Gamma x_{i+j} \neq 0 \end{cases} \quad \text{for } j \in \{0, \ldots, t+3\}.$$

Then the string of $t + 4$ bits

$$\gamma_i, \gamma_{i+1}, \ldots, \gamma_{i+t+3} \tag{6.2}$$

is called a *truncated linear trail* over t functions illustrated in Fig. 6.5. In the figure, $\gamma_{i+j} \in \{0, 1\}$, where $\gamma_{i+j} = 1$ indicates that the line is linearly active.

Like for differential trails, the propagation of differences through type-I and type-II GFNs with 4 lines with invertible functions is due to the following rules:

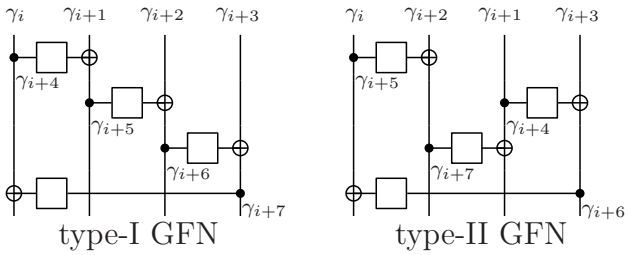

Figure 6.5: Truncated linear trails of type-I (4 rounds) and type-II (2 rounds) GFNs with 4 lines

Property 10 (**Linear zero rule for type-I GFN**). *If two of γ_i, γ_{i+1}, γ_{i+4} are zero, then all of them are zero, where $i = 0, 1, 2, \ldots$*

Property 11 (**Linear nonzero rule for type-I GFN**). *If γ_i, γ_{i+1}, γ_{i+4} are not all zero, at least two of them are nonzero, where $i = 0, 1, 2, \ldots$*

Property 12 (**Linear zero rule for type-II GFN**). *If two of γ_i, γ_{i+2}, γ_{i+5} are zero, then all of them are zero. Similarly, if two of γ_{i+1}, γ_{i+3}, γ_{i+4} are zero, then all of them are zero, where $i = 0, 2, 4, \ldots$*

Property 13 (**Linear nonzero rule for type-II GFN**). *If γ_i, γ_{i+2}, γ_{i+5} are not all zero, at least two of them are nonzero. Similarly, if γ_{i+1}, γ_{i+3}, γ_{i+4} are not all zero, at least two of them are nonzero, where $i = 0, 2, 4, \ldots$*

6.3.3 Active Functions and Equivalence for Type-I GFNs

With respect to differential cryptanalysis, we look for a tight lower bound on the number of differentially active functions among t consecutive functions of type-I GFN. In other words, for some positive number λ_δ, our aim is to prove

$$\sum_{j=3}^{t+2} \delta_{i+j} \geq \lambda_\delta, \tag{6.3}$$

where $i \geq 0$ and $t \geq 1$ (cf. Fig. 6.4). At the same time, a tight lower bound λ_γ on the number of linearly active functions among t functions means that (cf. Fig. 6.5)

$$\sum_{j=1}^{t} \gamma_{i+j} \geq \lambda_\gamma, \tag{6.4}$$

where $i \geq 0$ and $t \geq 1$. Direct manipulations with the indexes of δ_{i+j} and γ_{i+j} yield

Proposition 5. *Under the change of variables $\delta_{i+j} \mapsto \gamma_{i+t+3-j}$, $j \in \{0, \ldots, t+3\}$ the following holds for a 4-line type-I GFN with invertible functions:*

- *truncated differential trail* (6.1) *translates to truncated linear trail* (6.2)*,*
- *Property 6 translates to Property 10,*
- *Property 7 translates to Property 11, and*
- *if inequality* (6.3) *holds for $\lambda_\delta = \lambda$, then inequality* (6.4) *holds for $\lambda_\gamma = \lambda$.*

6.3.4 Active Functions and Equivalence for Type-II GFNs

Similarly to type-I GFNs, we explore tight lower bounds λ_δ and λ_γ on the number of differentially and linearly active functions among t functions of type-II GFN, i.e.:

$$\sum_{j=2}^{t+3} \delta_{i+j} \geq \lambda_\delta \tag{6.5}$$

and

$$\sum_{j=2}^{t+3} \gamma_{i+j} \geq \lambda_\gamma, \tag{6.6}$$

respectively, where $i \geq 0$ and $t \geq 2$ (see Figs. 6.4 and 6.5). Also here, we obtain the following

Proposition 6. *Under the change of variables $\delta_{i+j} \mapsto \gamma_{i+t+3-j}$, $j \in \{0, \ldots, t+3\}$ the following holds for a 4-line type-II GFN with invertible functions:*

- *truncated differential trail* (6.1) *translates to truncated linear trail* (6.2)*,*
- *Property 8 translates to Property 12,*
- *Property 9 translates to Property 13, and*
- *if inequality* (6.5) *holds for $\lambda_\delta = \lambda$, then inequality* (6.6) *holds for $\lambda_\gamma = \lambda$.*

Propositions 5 and 6 say that once we have a proof that the minimum number of differentially active functions among t consecutive functions of type-I and type-II GFNs with 4 lines is λ, we automatically obtain a proof that the minimum number of linearly active functions among t functions of the cipher is also λ.

6.4 Bounds for Active Functions

We focus on differentially active functions in this section, since one automatically obtains a proof for the minimum number of linearly active functions from a proof for the minimum number of differentially active functions as shown in the previous section (Propositions 5 and 6).

6.4.1 Some Truncated Differential Trails

Let *function i* of type-I or type-II GFN indicate the function whose output XOR-updates line number i. We refer to the XOR connecting to the i-th function's output as *the XOR of function i*. Then, if at least two of three lines connecting to the XOR of function i are non-active, the XOR is called *all-zero XOR*. Also, if at least one of the three lines connecting to the XOR of function i is active, the XOR is called *nonzero XOR*. These notions are related to Properties 6 to 9. For instance, when the XOR of function i of type-I GFN is all-zero, δ_i, δ_{i+3} and δ_{i+4} are all zero due to Property 6. Also, when the XOR of function i of type-II GFN is nonzero, at least two of δ_i, δ_{i+3}, δ_{i+5} are nonzero due to Property 9. Using these notions, the following truncated differential trails (treated as bit strings and $*$ denotes 0 or 1 in the strings) are derived:

GFN-I-1 (consecutive all-zero XORs). If the XORs of functions i and $i+1$ of type-I GFN are both all-zero, the forward and backward difference propagations will follow the truncated differential trail:

$$\delta_{i-7}\delta_{i-6}...\delta_i\delta_{i+1}...\delta_{i+8}\delta_{i+9} = 11 * 10110010001111.$$

Here $\delta_i = \delta_{i+3} = \delta_{i+4} = 0$ and $\delta_{i+1} = \delta_{i+4} = \delta_{i+5} = 0$ by assumption. $\delta_{i+2} = 1$ for invertibility. $\delta_{i+6} = 1$ due to Property 7, as $\delta_{i+2} = 1$. $\delta_{i+t} = 1$ for $t \in \{7, 8, 9\}$ is also due to Property 7, since $\delta_{i+t-1} = 1$ and $\delta_{i+t-4} = 0$. $\delta_{i-3} = 0$ due to Property 6, since $\delta_i = \delta_{i+1} = 0$. $\delta_{i-1} = \delta_{i-2} = 1$ due to Property 7, as $\delta_{i+1} = \delta_{i+3} = 0$ and $\delta_{i+2} = 1$. $\delta_{i-4} = \delta_{i-6} = 1$ for Property 7, since $\delta_i = \delta_{i-3} = 0$ and $\delta_{i-1} = \delta_{i-2} = 1$. $\delta_{i-7} = 1$ due to Property 7, since $\delta_{i-4} = 1$ and $\delta_{i-3} = 0$.

GFN-I-2 (no consecutive all-zero XORs). If the XOR of function i of type-I GFN is all-zero and there are no consecutive all-zero XORs, the forward and backward difference propagations will follow the truncated differential trail:

$$\delta_{i-4}\delta_{i-3}\delta_{i-2}\delta_{i-1}\delta_i\delta_{i+1}\delta_{i+2}\delta_{i+3}\delta_{i+4}\delta_{i+5} = 11 * 1011001.$$

Here $\delta_i = \delta_{i+3} = \delta_{i+4} = 0$ by assumption. The XORs of functions $i-1$ and $i+1$ are both nonzero. $\delta_{i+1} = \delta_{i+5} = 1$ due to Property 7, since $\delta_{i+4} = 0$. $\delta_{i-1} = \delta_{i+2} = 1$ is also due to Property 7, as $\delta_{i+3} = 0$. $\delta_{i-3} = \delta_{i-4} = 1$ is due to Property 7, as $\delta_i = 0$ and $\delta_{i+1} = \delta_{i-1} = 1$.

GFN-II-1 (consecutive all zero XORs in even numbered functions). If the XORs of functions i and $i+2$ of type-II GFN are both all-zero, the forward and backward difference propagations will follow the truncated differential trail:

$$\delta_{i-6}\delta_{i-5}...\delta_i\delta_{i+1}...\delta_{i+9}\delta_{i+10} = 1 * 111001001010111.$$

Here $\delta_i = \delta_{i+2} = \delta_{i+3} = \delta_{i+5} = \delta_{i+7} = 0$ by assumption. The XOR of function $i+1$ is not all zero for invertibility. $\delta_{i+1} = \delta_{i+4} = 1$ due to Property 9, since $\delta_{i+2} = 0$. $\delta_{i+6} = \delta_{i+9} = 1$ due to Property 9, since $\delta_{i+4} = 1$ and $\delta_{i+3} = \delta_{i+7} = 0$. $\delta_{i+8} = 1$ (Property 9), since $\delta_{i+6} = 1$ and $\delta_{i+5} = 0$. $\delta_{i+10} = 1$ (Property 9), since $\delta_{i+8} = 1$ and $\delta_{i+7} = 0$. $\delta_{i-1} = 0$ (Property 8). $\delta_{i-2} = \delta_{i-4} = 1$ (Property 9), as $\delta_{i+1} = 1$ and $\delta_{i-1} = \delta_{i+3} = 0$. $\delta_{i-3} = 1$ (Property 9), since $\delta_i = 0$ and $\delta_{i-2} = 1$. $\delta_{i-6} = 1$ (Property 9), as $\delta_{i-1} = 0$ and $\delta_{i-3} = 1$.

GFN-II-2 (consecutive all-zero XORs in odd numbered functions). If the XORs of functions $i+1$ and $i+3$ of type-II GFN are both all-zero, the forward and backward difference propagations will follow the truncated differential trail:

$$\delta_{i-5}\delta_{i-4}...\delta_i\delta_{i+1}...\delta_{i+10}\delta_{i+11} = 111011000010111 * 1.$$

Here $\delta_{i+1} = \delta_{i+2} = \delta_{i+3} = \delta_{i+4} = \delta_{i+6} = 0$ by assumption. $\delta_{i+5} = 1$ for invertibility. $\delta_{i+7} = \delta_{i+8} = 1$ due to Property 9, since $\delta_{i+2} = \delta_{i+6} = 0$ and $\delta_{i+5} = 1$. $\delta_{i+9} = 1$ due to Property 9, as $\delta_{i+4} = 0$ and $\delta_{i+7} = 1$. $\delta_{i+11} = 1$ for Property 9, since $\delta_{i+6} = 0$ and

$\delta_{i+9} = 1$. $\delta_i = 1$ (Property 9), since $\delta_{i+3} = 0$ and $\delta_{i+5} = 1$. $\delta_{i-2} = 0$ (Property 8), as $\delta_{i+1} = \delta_{i+3} = 0$. $\delta_{i-1} = \delta_{i-3} = 1$ (Property 9), since $\delta_{i+2} = \delta_{i-2} = 0$ and $\delta_i = 1$. $\delta_{i-4} = 1$ due to Property 9, as $\delta_{i+1} = 0$ and $\delta_{i-1} = 1$. $\delta_{i-5} = 1$ due to Property 9, since $\delta_{i-2} = 0$ and $\delta_{i-4} = 1$.

GFN-II-3 (no consecutive all-zero XORs in even and odd numbered functions). If the XORs of functions i of type-II GFN is all-zero and there is no consecutive all-zero XORs in even and odd numbered functions, the forward and backward difference propagations will follow the differential trail:

$$\delta_{i-3}\delta_{i-2}\delta_{i-1}\delta_i\delta_{i+1}\delta_{i+2}\delta_{i+3}\delta_{i+4}\delta_{i+5}\delta_{i+6}\delta_{i+7} = 1110110 * 0 * 1.$$

Here $\delta_i = \delta_{i+3} = \delta_{i+5} = 0$, and the XORs of functions $i-2$ and $i+2$ are both nonzero by assumption. The XOR of function $i+1$ is nonzero for invertibility. $\delta_{i+2} = \delta_{i+7} = 1$ for Property 9, since $\delta_{i+5} = 0$. $\delta_{i-2} = \delta_{i+1} = 1$ due to Property 9, as $\delta_{i+3} = 0$. $\delta_{i-1} = \delta_{i-3} = 1$ due to Property 9, since $\delta_i = 0$.

GFN-II-4 (no consecutive all-zero XORs in even and odd numbered functions). If the XORs of functions $i+1$ of type-II GFN is all-zero and there is no consecutive all-zero XORs in even and odd numbered functions, the forward and backward difference propagations will follow the truncated differential trail:

$$\delta_{i-4}\delta_{i-3}\delta_{i-2}\delta_{i-1}\delta_i\delta_{i+1}\delta_{i+2}\delta_{i+3}\delta_{i+4}\delta_{i+5}\delta_{i+6} = 1 * 1110010 * 1.$$

Here $\delta_{i+1} = \delta_{i+2} = \delta_{i+4} = 0$, and the XORs of functions $i-1$ and $i+3$ are both nonzero by assumption. The XOR of function i is nonzero for invertibility. $\delta_{i+3} = \delta_{i+6} = 1$ due to Property 9, since $\delta_{i+4} = 0$ and the XOR of function $i+3$ is nonzero. $\delta_i = \delta_{i-1} = 1$ due to Property 9, since $\delta_{i+2} = 0$ and the XOR of function $i-1$ is nonzero. $\delta_{i-2} = \delta_{i-4} = 1$ due to Property 9, since $\delta_{i+1} = 0$ and $\delta_{i+3} = \delta_{i-1} = 1$.

We also prove a proposition useful for demonstrating the minimum numbers of differentially active functions of type-I and type-II GFNs.

Proposition 7 (**Relation between active lines and nonzero XORs**). *For type-I and type-II GFNs with 4 lines and invertible functions, the number of active lines over t consecutive functions is greater or equal to the number of nonzero XORs over t consecutive functions plus one, given a nontrivial input difference.*

Proof. Since any two sets of lines connecting to two nonzero XORs have at most one overlapping line from Property 7 or 9, the number of active lines is bounded by the number of nonzero XORs. □

We employ the above bit strings and Proposition 7 to prove the minimum number of differentially active functions of type-I and type-II GFNs in the following subsections.

6.4.2 Differentially Active Functions of Type-I GFNs

Lemma 4. *For 4-line type-I GFNs with invertible functions, every nontrivial differential trail over 14 rounds with at most 4 all-zero XORs has at least 7 active functions.*

Proof. Since at least $14 - 4 = 10$ XORs over 14 rounds are nonzero, there exist at least 11 active lines from Proposition 7. Up to 4 of active lines are not counted, since the corresponding differences do not enter any functions within the 14 rounds. This gives at least $11 - 4 = 7$ nonzero active lines and at least 7 active functions. □

Lemma 5. *For 4-line type-I GFNs with invertible functions, every nontrivial differential trail over 14 rounds with consecutive all-zero XORs has at most 4 all-zero XORs.*

Proof. From the string GFN-I-1, the XOR of function $i - 3$ is all-zero assuming that the XORs of functions i and $i + 1$ are all zero. The other XORs starting from function $i - 11$ to $i + 9$ are nonzero. In the backward difference propagation, the first possible all-zero XOR appears in function $i - 12$. Thus, there are at most 4 all-zero XORs in the backward direction. Since the XORs of functions j and $j + 2$ cannot be all-zero simultaneously for any j due to the invertibility, there are at most 2 all-zero XORs of function $i + 10$ to $i + 13$. Therefore, there are at most 4 all-zero XORs in the forward direction. □

Lemma 6. *For 4-line type-I GFNs with invertible functions, every nontrivial differential trail over 14 rounds without consecutive all-zero XORs has at most 4 all-zero XORs.*

Proof. From the string GFN-I-2, the XORs of functions $i - 8$ to $i - 1$, as well as functions $i + 1$, $i + 2$ and $i + 5$ are nonzero, assuming that the XOR of function i is all-zero and there is no consecutive all-zero XORs. If the XOR of function $i + 3$ is all-zero, $\delta_{i+6} = \delta_{i+7} = 0$ due to Property 6. In that case, the XOR of function $i + 4$ is also all-zero due to Property 6, since $\delta_{i+4} = \delta_{i+7} = 0$, and this contradicts the assumption. Thus, the XOR of function $i + 3$ is nonzero. Then $\delta_{i+6} = \delta_{i+7} = \delta_{i+8} = 1$ due to Property 7, since $\delta_{i+3} = \delta_{i+4} = 0$. Therefore the XORs of functions $i + 1$ to $i + 8$ are nonzero. Since there are at most three all-zero XORs in any five consecutive rounds assuming that there is no consecutive all-zero XORs, there are at most four all-zero XORs in the forward and backward directions. □

Lemmata 4 to 6 yield

Proposition 8 (**Active functions for type-I GFNs**). *The 4-line type-I GFN with invertible functions provides at least 7 differentially active functions over 14 consecutive rounds for each non-trivial input difference.*

6.4.3 Differentially Active Functions of Type-II GFNs

Lemma 7. *For 4-line type-II GFNs with invertible functions, every differential trail over 6 rounds with at most 3 all zero XORs has at least 6 active functions.*

Proof. Since at least $12 - 3 = 9$ XORs over 6 rounds are nonzero, there exist at least 10 active lines from Proposition 7. Up to 4 of active lines are not counted, since the corresponding differences do not enter any functions within the 6 rounds. This gives at least $10 - 4 = 6$ nonzero active lines and at least 6 active functions. □

Lemma 8. *For 4-line type-II GFNs with invertible functions, every nontrivial differential trail over 6 rounds with consecutive all-zero XORs in even numbered functions has at most 3 all-zero XORs.*

Proof. From the string GFN-II-1, the XORs starting from function $i-9$ to $i-2$, $i+1$, from $i+3$ to $i+10$ are nonzero, assuming that the XORs of functions i and $i+2$ are all-zero. Thus, there are at most three all-zero XORs in both directions. □

Lemma 9. *For 4-line type-II GFNs with invertible functions, every nontrivial differential trail over 6 rounds, with consecutive all-zero XORs in odd numbered functions has at most 3 all-zero XORs.*

Proof. From the string GFN-II-2, the XORs of functions $i-8$ to $i-3$, functions $i-1$, i, $i+2$, as well as functions $i+4$ to $i+9$, and $i+11$ are nonzero, assuming that the XORs of functions $i+1$ and $i+3$ are all-zero. Thus, there are at most three all-zero XORs in both directions. □

Lemma 10. *For 4-line type-II GFNs with invertible functions, every nontrivial differential trail over 6 rounds, without consecutive all-zero XORs in both even numbered rounds and odd numbered rounds has at most 3 all-zero XORs.*

Proof. Consider the following two cases.

case 1. If the XOR of function i is nonzero, then the XORs of functions $i-6$ to $i-1$ as well as functions $i+1$, $i+2$, $i+4$, and $i+7$ are nonzero from the string GFN-II-3. If the XOR of function $i+3$ is all-zero, then $\delta_{i+4} = \delta_{i+6} = 0$ due to Property 8. Since $\delta_{i+5} = \delta_{i+6} = 0$, the XOR of function $i+5$ is also all-zero due to Property 8 and this contradicts the assumption. Thus, the XOR of function $i+3$ is nonzero. Then $\delta_{i+4} = \delta_{i+6} = 1$ due to Property 9, and $\delta_{i+8} = 1$ due to Property 9, since $\delta_{i+5} = 0$ and $\delta_{i+6} = 1$. Therefore, the XORs of functions $i+1$ to $i+8$ are nonzero. Since the XORs of functions $i-6$ to $i-1$ are nonzero, there are at most one all-zero XOR in any 7 consecutive functions in both directions. Thus, there are at most three all-zero XORs in any 12 consecutive functions.

case 2. If the XOR of function $i+1$ is nonzero, then the XORs of functions $i-7$ to i as well as functions $i+3$, $i+5$, and $i+6$ are nonzero. If the XOR of function $i+2$ is all-zero, $\delta_{i+5} = \delta_{i+7} = 0$ due to Property 8. Since $\delta_{i+4} = \delta_{i+7} = 0$, the XOR of function $i+4$ is also all-zero due to Property 8 and this contradicts the assumption. Thus, the XOR of function $i+2$ is nonzero. Then $\delta_{i+5} = \delta_{i+7} = 1$ due to Property 9, since $\delta_{i+2} = 0$. Also, the XOR of function $i+4$ is nonzero, since $\delta_{i+7} = 1$. Since the XORs of functions $i-7$ to i and functions $i+2$ to $i+7$ are nonzero, there is at most one all-zero XOR in any 7 consecutive functions in both directions. Thus, there are at most three all-zero XORs in any 12 consecutive functions.

□

Again, Lemmata 7 to 10 yield

Proposition 9 (**Active functions for type-II GFNs**). *The 4-line type-II GFN with invertible functions provides at least 6 differentially active functions over 6 rounds for each non-trivial input difference.*

6.4.4 Active Functions for Contracting GFNs

We do not have tight lower bounds on the number of active functions for the contracting GFNs due to those complicated structures. However, we have exhaustively searched the number of active functions up to 50 rounds for all contracting GFNs classified in this chapter. In these experiments, we observe that only 2 of contracting GFNs (GFN2.3 and GFN2.4 in Fig. 6.3 have slightly larger number of active functions than non-contracting GFNs. Both structures exhibit strong differential effects though.

For Nyberg's GFN with 4 lines [Nyb96] (GFN2.8 in Fig. 6.3), the numerical results show that about 1/3 of the round functions are active up to 50 rounds. Recall that it is 1/2 for type-I/II GFNs. This implies that not only GFN2.8 exhibits a differential effect but also the proportion of active functions in all functions is lower for it, resulting in a lower efficiency.

6.4.5 Application to SHAvite-3_{512}

Proposition 9 also directly applies to the block cipher E^{512} underlying the compression function C^{512} of the second-round SHA-3 candidate SHAvite-3_{512} and significantly improves the upper bound on the differential trail probability in Lemma 5 of [DB09]. While [DB09] shows that 9 rounds of E^{512} have at least 6 active functions and a maximum differential trail probability of 2^{-678} for each nontrivial input difference, Proposition 9 implies that already 6 rounds of 4-line SHAvite-3_{512} provide at least 6 active functions. Therefore 9 rounds of E^{512} have at least 8 active functions, since the remaining 3 rounds provide at least two more active functions, and give a maximum differential trail probability of 2^{-904}.

6.5 Comparative Efficiency of GFNs

6.5.1 Converting Active Functions to Active S-Boxes

Linear transforms M with the highest branch number can be built from the generator matrices of maximum distance separable codes and are called *MDS*. Note that, for GFNs utilizing SP-functions with the diffusion matrix M, $\mathcal{B}(M)$ and $\mathcal{B}({}^tM)$ imply the diffusion property for differential and linear attacks, respectively [Kan00, Shi10], where ${}^tM$ is the transpose matrix of M.

When a type-I or type-II GFN is instantiated with SPS-functions or double SP-functions, the minimum number of differentially and linearly active functions directly translates to a lower bound on the number of differentially and linearly active S-boxes, unlike the Feistel constructions with single SP-functions for which quite involving techniques are usually necessary at this point. We formulate this formally as

Proposition 10 (**Active functions to active S-boxes**). *Let $\mathcal{B}$ be the branch number of the diffusion matrix M or its transpose ${}^tM$. Whenever a function is active (differentially or linearly) in type-I or type-II GFNs with SPS-functions or double SP-functions, it provides at least $\mathcal{B}$ (differentially or linearly) active S-boxes.*

Combining Proposition 10 with Propositions 8 and 9 gives the minimum number of differentially active S-boxes for type-I and type-II GFNs. Then the equivalence between

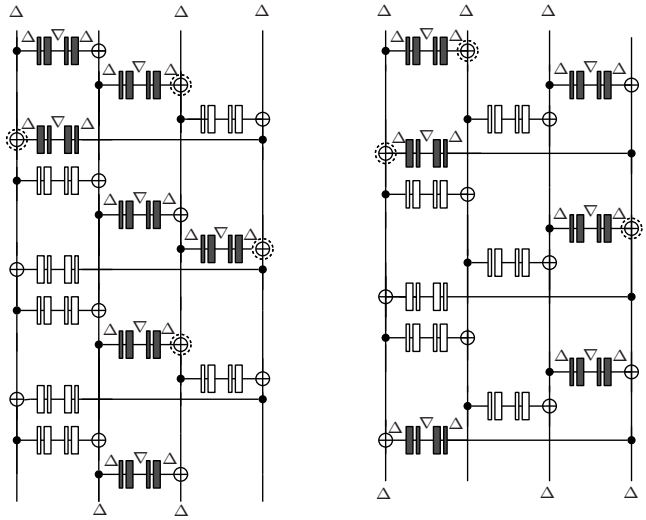

Figure 6.6: Truncated differential trails of 4-line type-I (14 rounds) and type-II (6 rounds) GFNs with double SP-functions attaining the lower bounds of Theorems 4 and 5

differential and linear cryptanalysis (Propositions 5 and 6) yields the minimum number of linearly active S-boxes. Thus, one directly obtains:

Theorem 4 (**Active S-boxes for type-I GFNs**). *For each nontrivial differential or linear trail, every* $14R$*,* $R \geq 1$*, rounds of 4-line type-I GFN with SPS-functions or double SP-functions provide at least* $7\mathcal{B}R$ *active S-boxes (differentially or linearly), where* $\mathcal{B}$ *is the branch number of the diffusion matrix or its transpose in the SP-functions.*

Theorem 5 (**Active S-boxes for type-II GFNs**). *For each nontrivial differential or linear trail, every* $6R$*,* $R \geq 1$*, rounds of 4-line type-II GFN with SPS-functions or double SP-functions provide at least* $6\mathcal{B}R$ *active S-boxes (differentially and linearly), where* $\mathcal{B}$ *is the branch number of the diffusion matrix or its transpose in the SP-functions.*

Theorems 4 and 5 can be seen as the main results of this chapter. The lower bounds on the number of active functions translate to upper bounds on the differential and linear trail probabilities in a standard way: If p and q are the maximum linear and differential probabilities of the S-boxes, the probability of a $14R$-round nontrivial linear and differential trail will be upper-bounded by $p^{7\mathcal{B}R}$ and $q^{7\mathcal{B}R}$, respectively, for type-I GFNs. For type-II GFNs, the probability of a $6R$-round nontrivial differential and linear trail will be upper-bounded by $p^{6\mathcal{B}R}$ and $q^{6\mathcal{B}R}$, respectively.

6.5.2 Tightness of Bounds

The lower bounds of Theorems 4 and 5 on the number of active S-boxes are actually tight, since there exist S-box truncated trails attaining those minimal numbers. In Fig. 6.6, we demonstrate a 14-round differential trail for type-I and a 6-round differential trail for type-II GFNs with double SP-functions and MDS diffusion having $7(m+1)$ and $6(m+1)$ active S-boxes, respectively. Note that the input and output differences for each of the

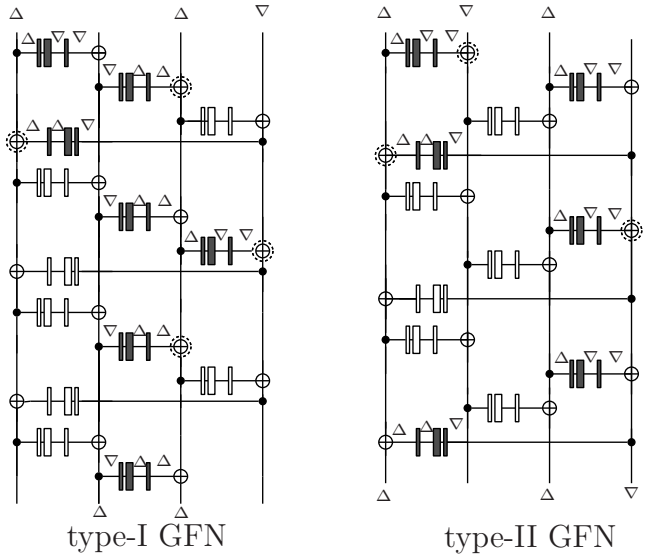

Figure 6.7: Truncated differential trails of 4-line type-I (14 rounds) and type-II (6 rounds) GFNs with SPS-functions attaining the lower bounds of Theorems 4 and 5

functions active in the trails contain exactly one active component. At the same time the internal difference in each of them involves all S-boxes. In the figure, Δ and ∇ denote S-box truncated difference 100...00 (only the first S-box active out of m) and 111...11 (all m S-boxes active), respectively. Note that the trail for type-II GFN is iterative. XORs with difference cancellation are marked with dashed circles.

While the 6-round trail for type-II GFNs is iterative and illustrates the tightness of Theorem 5 for any R, there are no iterative trails for 14 rounds of type-I GFNs with exactly $7(m+1)$ active S-boxes. However, we successfully verified that for up to 56 rounds of type-I GFNs there are non-iterative trails exactly achieving the lower bound on the number of active S-boxes of Theorem 4. Similarly, a 14-round differential trail for type-I and a 6-round differential trail for type-II with SPS-functions and MDS diffusion having $7(m+1)$ and $6(m+1)$ active S-boxes are illustrated in Fig. 6.7, respectively.

6.5.3 GFNs: SPS-Functions or Double SP-Functions vs Single SP-Functions

Now we can compare type-I and type-II GFNs with single and SPS-functions or double SP-functions with respect to the efficiency metrics $\mathcal{E}$ and $\mathcal{E}_m$. The usefulness of these metrics is not limited to reflecting the time performance of some software implementations. We also expect it to indicate efficiency regarding such crucial parameters as energy and area consumption of a design in hardware.

Recall that bundle size m is the number of components in each of the 4 lines of the cipher constructions under consideration. We perform comparison for MDS diffusion matrix M, i.e. for $\mathcal{B}(M) = m+1$. The results are given in Table 6.2 and Fig. 6.8.
Figure 6.8 shows $\mathcal{E}_m$ for type-I and type-II GFNs with 4 lines, where absolute values of $\mathcal{E}_m$ (on the left) and normalized advantage of SPS-functions or double SP-functions

Table 6.1: Efficiency $\mathcal{E}$ of 4-line GFNs with single and invertible SPS-functions or double SP-functions using MDS diffusion matrices with respect to differential and linear cryptanalysis, see also Figs. 6.1 and 6.2

	type-I GFN			type-II GFN		
	$\mathcal{E}$	$\mathcal{E}_4$	$\mathcal{E}_8$	$\mathcal{E}$	$\mathcal{E}_4$	$\mathcal{E}_8$
single SP	0.188 [WZL06]	0.250 [WZL06]	0.219 [WZL06]	0.167 [Shi10]	0.229 [Shi10]	0.198 [Shi10]
SPS or double SP (this chapter)	0.250	0.313	0.281	0.250	0.313	0.281
advantage of SPS or double SP	33.3%	25.0%	28.3%	50.0%	36.7%	41.9%

Table 6.2: Efficiency metrics $\mathcal{E}_m$ and $\mathcal{E}$ for 4-line type-I and type-II GFNs with MDS diffusion: single SP-functions vs SPS-functions or double SP-functions, see also Fig. 6.8

	r	$A_{m,r}$	$S_{m,r}$	$\mathcal{E}_m$	$\mathcal{E}$
GFN-I, single SP [WZL06]	$16R$	$[3(m+1)+1]R$	$16mR$	$\frac{3m+4}{16m}$	3/16
GFN-II, single SP [Shi10]	$6R$	$[2(m+1)+2]R$	$12mR$	$\frac{2m+3}{12m}$	1/6
GFN-I, SPS or double SP (Th. 4)	$14R$	$[7(m+1)]R$	$28mR$	$\frac{m+1}{4m}$	1/4
GFN-II, SPS or double SP (Th. 5)	$6R$	$[6(m+1)]R$	$24mR$	$\frac{m+1}{4m}$	1/4

over single SP-functions (on the right). As one can see from Fig. 6.8, type-I and type-II GFNs perform consistently better with SPS-functions or double SP-functions than with single SP-functions with respect to $\mathcal{E}_m$ for all block sizes. For short blocks ($m = 2$), the advantage is at least 20% for type-I GFN and at least 28% for type-II GFN. For longer blocks ($m = 32$), $\mathcal{E}_m$ becomes close to $\mathcal{E}$ and the advantage amounts to about 33% and 50%, respectively. These results show that the instantiation with the SPS-functions or double SP-functions can more than halve the required number of rounds compared to that with the single SP-function. This implies that the SPS construction or double SP construction is still more efficient than the single SP construction, even if a single round computation of the SPS or double SP is twice as slow as that of the single SP. That is to say, our results are not a tradeoff between the number of S-boxes in a single-round and the required number of rounds. See also Table 6.1.

Furthermore, we compare with the efficiency for 4-line type-I and type-II GFNs using multiple-round diffusion with optimal diffusion matrices [SA08], or diffusion-switching mechanism [SS04]. We first compare the efficiency obtained from the proven bounds, and then compare the efficiency derived from experiments with some concrete parameters for a more accurate consideration. Generally speaking, it is hard to directly compare the efficiency of 4-line type-I and type-II GFNs with SPS or double SP to those with SP using multiple-round diffusion and optimal diffusion matrices (SP-M), since there are no

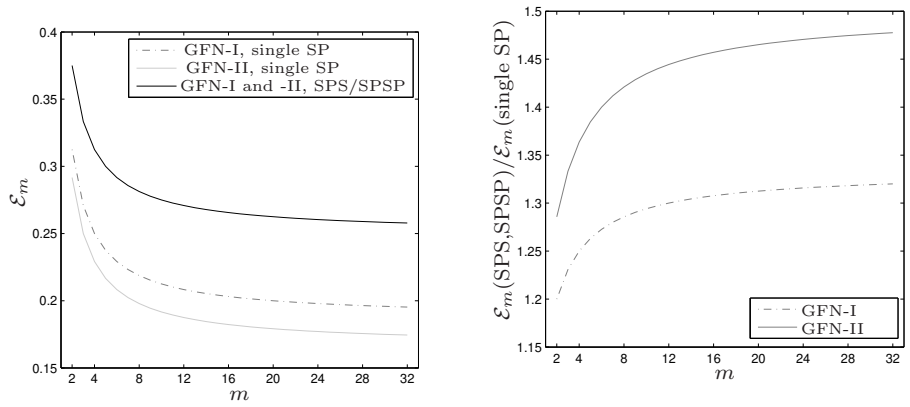

Figure 6.8: Efficiency metric $\mathcal{E}_m$ for type-I and type-II GFNs with 4 lines

tight proven bounds for the latter case.

$\mathcal{E}_m$ given by Theorems 1 to 4 of [SA08] for type-I and type-II GFNs is $(m+1)/6m$ for both differentially and linearly active S-boxes (i.e. $\mathcal{E}_4 = 0.208$, $\mathcal{E}_8 = 0.188$, and $\mathcal{E} = 0.167$). According to these proven bounds, a comparison of these values to Tables 6.1 and 6.2 yields that type-I and type-II GFNs with SPS-functions or double SP-functions and single-round diffusion are much more efficient than the respective constructions with single SP-functions and multiple-round diffusion.

Again, we note that the proven bounds of [SA08] do not appear to be tight [WB12]. That is why we do not include this consideration into Table 6.2 and Fig. 6.8. On the other hand, from our numeric search results, the efficiency of SP-M seems similar to that of SPS or double SP after a certain number of rounds, being much higher than that of the constructions with SP-functions and single-round diffusion. We provide Fig. 6.9 that shows the non-asymptotic efficiency $\mathcal{E}_{m,r}$ regarding the number of differentially active S-boxes up to 24 rounds for the 4-line type-II GFNs with SPS, double SP or SP-M for $m \in \{4, 8\}$. $\mathcal{E}_{m,r}$ for the SPS or double SP construction is derived from Theorem 5 and that for the SP-M construction is obtained by the numeric search. While the numeric results show much higher efficiency compared to the proven bounds for SP-M, the SPS or double SP constructions are slightly more efficient than the SP-M constructions at least up to 24 rounds. In addition, the SP-DSM construction has twice more permutation layers to guarantee a similar number of active S-boxes and needs to maintain at least two different matrices, which may reduce the efficiency in practice.

6.5.4 GFNs vs SPNs

While the efficiency metric $\mathcal{E}_m$ for type-I and type-II GFNs with SPS-functions or double SP-functions is higher than that of the other GFNs, it is likely to be lower than that for SPN structures. For example, it is well-known [DR02] that 4 rounds of AES have 64 S-boxes and at least 25 active S-boxes and that this bound is actually tight. Since 1-round of AES is comparable to 4 SP-functions consisting of 4 S-boxes in each S-box layer and MDS matrix in terms of computational effort, $\mathcal{E}_4$ of AES is about 0.391. However, GFNs have distinctive features such as involution property. Thus, if decryption is needed, GFNs

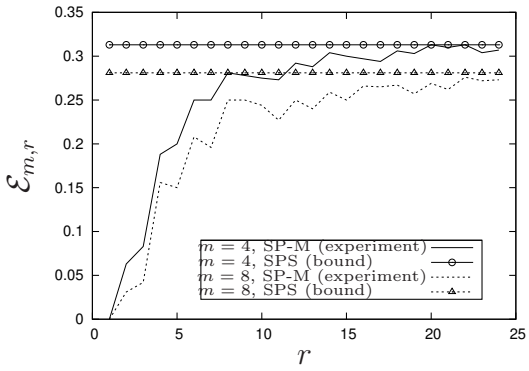

Figure 6.9: Experimental efficiency $\mathcal{E}_{m,r}$ (regarding the number of differentially active S-boxes) and bounds for type-II GFNs with 4 lines and $m \in \{4, 8\}$.

are easier to invert, whereas inverting SPN structures is usually more involving and can imply some performance penalty.

6.6 Further Analysis of GFNs

6.6.1 Other Attacks

Given the scale of popularity of GFNs among the designers of symmetric primitives, it is no surprise that also analysis approaches other than differential and linear cryptanalysis have been applied to evaluate the security of GFN constructions. Interestingly, it was the publication of the GFN-like construction Skipjack that stipulated the *impossible differential cryptanalysis* [BBS99], [BKR97] that was successfully applied to round-reduced AES [Pha04], [LDKK08] afterwards. For most Feistel structures with invertible functions, relatively long impossible differentials are known. For instance, BFN has a 5-round impossible differential. Type-I and type-II GFNs with 4 lines have 19- and 9-round impossible differentials, respectively [CY09, TTS+08]. Attack approaches based on impossible differential cryptanalysis can often break more rounds of GFN-based ciphers than any other type of cryptanalysis. This motivated [SM10], where approaches have been proposed to limit the length of impossible differentials for type-II GFNs by choosing alternative types of line-shuffling between the rounds. However, in the case of GFNs with 4 lines, which is our major focus in this work, no improved shuffling exists. *Zero-correlation linear cryptanalysis* [BR14, BW12], can be seen as the counterpart of impossible differential cryptanalysis in the domain of linear cryptanalysis. In most cases, the length of the longest zero-correlation linear hulls for GFNs is comparable to that of the longest known impossible differentials.

Cancellation cryptanalysis [BDLF10] is a recent attack technique applicable to GFN-type hash functions. Cancellation cryptanalysis turns into a saturation attack [BDLF10] when applied to the block cipher underlying the Lesamnta hash function [HKY00]. However, the attack relies on a subkey-collision effect and its complexity essentially depends on the fact that there is only limited amount of key material input into each function. Thus, the cancellation cryptanalysis quickly becomes less efficient, once several subkeys

are introduced in each function, as it is the case for the type-I and type-II GFNs with SPS-functions or double SP-functions.

6.6.2 Differential and Linear Probability of GFNs with SPS-Functions or Double SP-Functions

We consider the provable security of the 4-line type-II GFNs with SPS-functions against differential and linear attacks in this section in terms of maximum average differential and linear probabilities. Many differential trails can contribute to the same differential. Similarly, many linear trails will have their non-zero contributions to the same linear hull probability. As these probabilities of the type-I GFNs have not been studied so far, we only deal with type-II GFNs here.

The maximum differential and the maximum average linear probabilities for SPNs were discussed in [HLL$^+$00]. According to these results, the maximum differential and the maximum linear hull probabilities for one SPS-function (called SDS function in [HLL$^+$00]), assuming that the underlying diffusion matrix is MDS, are p^m and q^m, where p and q are the maximum differential and the maximum linear probability for each S-box, respectively, and m is the number of S-box in a substitution layer. These bounds might be slightly improved depending on the elements of the diffusion matrix and the S-box [PSC$^+$02, PSLL03].

The provable security for the type-II GFNs with 4 lines against differential and linear attacks was discussed in [KLS$^+$08]. It has been shown that the probability of each differential and linear hull of type-II GFNs with 4 lines (called CLEFIA structure in [KLS$^+$08]) over 5 rounds are bounded by $\mathcal{P}^4 + 2\mathcal{P}^5$ and $\mathcal{Q}^4 + 2\mathcal{Q}^5$, where $\mathcal{P}$ and $\mathcal{Q}$ are the maximum differential and the maximum linear hull probability for each F-function, respectively. Then, the bound for the security against differential attack was improved to $\mathcal{P}^4 + \mathcal{P}^5$ by [MSS11]. Combining those results directly yields the following upper bounds:

Theorem 6. *The average differential probability of the 4-line type-II GFN with SPS-functions or double SP-functions over 5 rounds is upper-bounded by $p^{4m} + p^{5m}$, assuming that the provided round keys are independently and uniformly distributed.*

Theorem 7. *The average linear probability of the 4-line type-II GFN with SPS-functions or double SP-functions over 5 rounds is upper-bounded by $q^{4m} + 2q^{5m}$, assuming that the provided round keys are independently and uniformly distributed.*

As discussed in Section 6.5.1, for type-II GFNs with SPS-functions or double SP-functions, the probability of a 6-round nontrivial differential and linear trail are bounded by $p^{6(m+1)}$ and $q^{6(m+1)}$, respectively. Thus, gaps between the proven bounds on the maximum differential (linear) probability and the maximum differential (linear) characteristic probability for the 4-line type-II GFN with SPS-functions or double SP-functions appear to be relatively small. For instance, suppose that the underlying S-box and diffusion matrix are the AES S-box and matrix, i.e., a 128-bit block cipher with $m = 4$ and $p = q = 2^{-6}$. In this case, the differential and the linear hull probabilities of the GFN with SPS-functions or double SP-functions over 5 rounds are upper-bounded by $2^{-96} + 2^{-120}$ and $2^{-96} + 2^{-119}$, respectively.

6.7 Conclusions

In this chapter, we have discussed the classification, security and efficiency of 4-line GFNs. We provide a definition of a GFN and demonstrate that there are only 2 non-contracting representatives in the class of 4-line GFNs up to equivalence, namely, the type-I and type-II GFNs that avoid obvious differential effects. Moreover, we propose to instantiate the GFNs with SPS-functions or double SP-functions instead of single SP-functions and show that the instantiation with SPS-functions or double SP-functions using MDS diffusion provides a proportion of differentially and linearly active S-boxes by up to 33% and 50% higher than that with single SP-functions for type-I and type-II GFNs, respectively, if the same matrix is used in all rounds. This opens up the possibility of designing more efficient block ciphers based on GFN structure.

Chapter 7

Optimal Design of Balanced Feistel Networks with Substitution-Permutation Functions

7.1 Introduction

Balanced Feistel networks (BFNs) are one of the most widely used structures for a block cipher. However, the optimal design strategy with respect to both the security and the efficiency for its F-function is still an open problem. This chapter addresses this problem in a wide class of typical underlying functions for a BFN (substitution-permutation functions with any finite number of layers). To do that, for each of them, we first prove tight bounds on the security parameter (number of active S-boxes). Then the security parameter is related to the computational workload of a cipher implementation (modelled as the number of S-boxes computed in the cipher) to obtain an efficiency parameter. Finally, the optimal constructions are those with the maximum resulting efficiency parameter.

The class of ciphers. We focus on balanced Feistel networks with SP-type bijective F-functions defined in Section 3.1. We treat F-functions with $(\mathrm{SP})^{2t}$, $(\mathrm{SP})^{2t+1}$, $(\mathrm{SP})^{2t-1}\mathrm{S}$ and $(\mathrm{SP})^{2t}\mathrm{S}$-type F-functions for an integer $t \geq 1$. For instance, an $(\mathrm{SP})^{2}\mathrm{S}$-type F-function consists of two consecutive SP-functions followed by an S-box layer, namely an SPSPS F-function.

Security parameter. Counting the *minimum number of active S-boxes* is a widely accepted argument [DR02] to demonstrate the immunity of a cryptographic algorithm against differential [BS91] and linear [Mat93] cryptanalysis which are two fundamental attacks on block ciphers. Lower bounds on the number of active S-boxes are closely related to the probability of differential trails and linear trails [DR02].

For each of the BFN instantiations above, we prove lower bounds on the number of differentially and linearly active S-boxes. In contrast to the previous works [Kan00] and [Bog10], our results with respect to this security parameter:

- generalize the type of the F-function, while [Kan00] and [Bog10] only contain lower bounds for BFNs with SP- and SPS- functions,
- hold for any number of rounds (those of [Kan00] and [Bog10] hold only for a few rounds), and

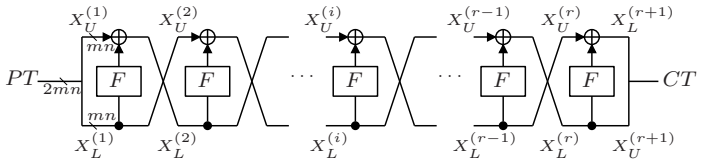

Figure 7.1: r-round BFN with bijective F-functions

- contain proofs of tightness for the bounds when the matrices used in the diffusion layers of BFNs are *maximum distance separable* (MDS).

Efficiency metric.

To measure the efficiency of a construction, we are using the ratio between active S-boxes and all S-boxes in a cipher $\mathcal{E}_m$ defined in Section 3.2.2.

Optimality. In the wide class of our target ciphers, we prove optimality of several instances with respect to the efficiency parameter. More specifically, among BFN block ciphers with bijective SP-type F-functions and MDS diffusion, we prove *BFNs with SPS and SPSP functions to maximize the efficiency* in terms of the proportion of active S-boxes in all S-boxes. Interestingly, one SP-layer in the function is not enough to attain optimality, whereas taking more than two S-box layers does not increase the efficiency either.

Organization of the chapter. The remainder of this chapter is organized as follows. Section 7.2 describes the target structure and definitions. The duality of differential and linear trails is explained in Section 7.3. Section 7.4 gives proofs for lower bounds on the numbers of differentially and linearly active S-boxes for the BFNs and its results are summarized in Table 7.1. Section 7.5 shows the tightness of those bounds. Section 7.6 discusses the optimality of the BFNs. Finally, we conclude in Section 7.7.

7.2 Preliminaries

7.2.1 Target Structures

In this chapter, we focus on balanced Feistel networks (BFNs) with bijective F-functions defined in Section 3.1. As a reminder, our target structures in this chapter are described in Fig. 7.1. Note that, instead of $x_0^{(i)}$ and $x_1^{(i)}$, we use $X_L^{(i)}$ and $X_U^{(i)}$ as the notations for the left half and right half of the i-th round input, respectively, in this chapter. While mn-bit subkeys are XORed before each S-box layer, we omit these subkey additions in this chapter for simplicity. An S-box layer consists of m n-bit bijective S-boxes, and a linear diffusion layer consists of mn-bit linear Boolean function. BFN-$(\mathrm{SP})^u$ denotes BFN with F-functions consisting of u consecutive SP-functions. BFN-$(\mathrm{SP})^u$S denotes BFN with F-functions consisting of u consecutive SP-functions followed by one additional S-box layer. See Figs. 7.1 and 7.2.

7.2.2 Notations

We use the following notations throughout this chapter:

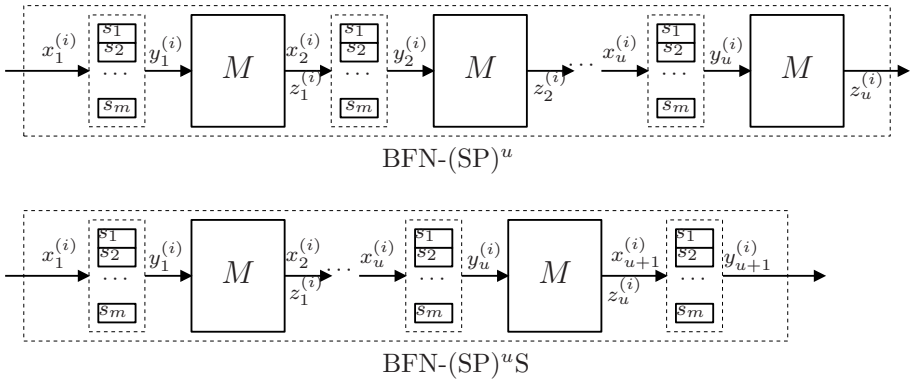

Figure 7.2: The i-th round F-function of BFN-(SP)^u and BFN-(SP)^{u}S.

- $x_j^{(i)}, y_j^{(i)}$: input and output of the j-th S-box layer in the i-th round.
- $z_j^{(i)}$: output of the j-th linear diffusion layer in the i-th round.
- $\Delta x_j^{(i)}$: a difference of $x_j^{(i)}$.
- $dw_j^{(i)}$: a truncated difference weight of $x_j^{(i)}$, i.e., $dw_j^{(i)} = w_n(\Delta x_j^{(i)})$.
- $dw^{(i)}$: the number of differentially active S-boxes in the i-th round.
- $\mathcal{D}(r)$: the minimum number of active S-boxes in r consecutive rounds.
- $\Gamma y_j^{(i)}$: a linear mask value of $y_j^{(i)}$.

7.3 Duality of Trails

In this section, we demonstrate an equivalence between differential and linear trails for the BFNs. This equivalence follows from Biham's considerations in [Bih94] and is provided here for completeness. It allows us to work with the minimum numbers of differentially and linearly active S-boxes simultaneously. We first show an equivalent transform for BFN-(SP)^u.

Property 14. *Suppose that both S-box layer and linear diffusion layer are bijective. Any BFN consisting of u consecutive SP-functions, BFN-(SP)^u, can be equivalently transformed into a BFN consisting of u consecutive PS-functions with an initial and a final linear function.*

This property is seen as a generalization of [Kan00]. Let $v_j^{(i)} = P^{-1}(x_j^{(i)})$. From the definition, $P(y_u^{(i)}) = x_1^{(i-1)} \oplus x_1^{(i+1)}$, then $y_u^{(i)} = P^{-1}(x_1^{(i-1)} \oplus x_1^{(i+1)})$. Since P is linear, $y_u^{(i)} = v_1^{(i-1)} \oplus v_1^{(i+1)}$. Meanwhile, $y_u^{(i)} = S(P(S(\cdots P(S(x_1^{(i)}))\cdots)))$, then $y_u^{(i)} = S(P(S(\cdots P(S(P(v_1^{(i)})))\cdots)))$. Combining the above equations, $v_1^{(i+1)} = S(P(S(\cdots P(S(P(v_1^{(i)})))\cdots)) \oplus v_1^{(i-1)}$. Now we have BFN-(PS)^u from BFN-(SP)^u by using equivalent transforms. Note

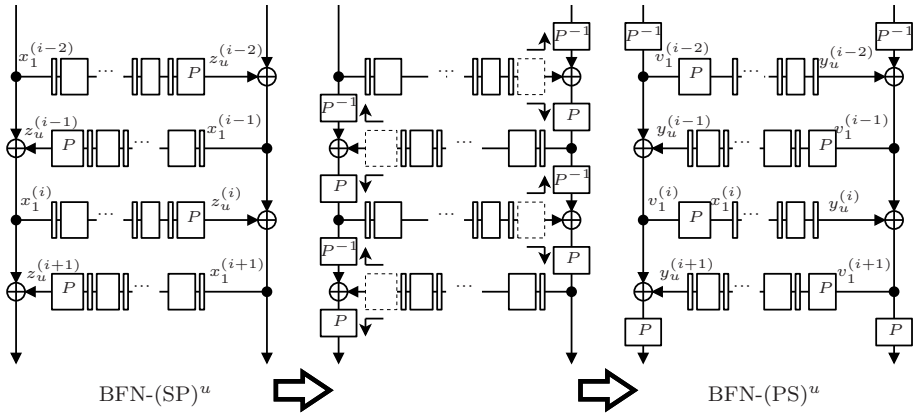

Figure 7.3: Equivalent transform (BFN-(SP)^u to BFN-(PS)^u), where thin boxes and thick boxes denote S-box layers and P-layers, respectively.

that BFN-(PS)^u takes $\mathcal{P}' = (P^{-1}(X_L^{(1)}),\ P^{-1}(X_U^{(1)}))$ as a plaintext and outputs a ciphertext $\mathcal{C}' = (P(X_U^{(r+1)}), P(X_L^{(r+1)}))$. Since these initial and final linear functions do not affect the minimum numbers of active S-boxes, we can ignore these functions when studying the minimum numbers of active S-boxes. An illustration of these equivalent transforms is given in Fig. 7.3.

From the concatenation rules [Bih94, Mat94], $\Gamma v_1^{(i)} = \Gamma y_u^{(i-1)} \oplus \Gamma y_u^{(i+1)} = {}^tP(\Gamma x_1^{(i)})$, where ${}^tP$ is the bit-based transpose matrix of P. Thus, for BFN-(SP)^u, the linear trails can be transformed to the corresponding differential trails by replacing ($\Delta x_1^{(i)}$, $\Delta x_2^{(i)}$, ..., $\Delta x_u^{(i)}$), ($\Delta z_1^{(i)}$, $\Delta z_2^{(i)}$, ..., $\Delta z_u^{(i)}$) and P with ($\Gamma y_u^{(i)}$, $\Gamma y_{u-1}^{(i)}$, ..., $\Gamma y_1^{(i)}$), ($\Gamma v_u^{(i)}$, $\Gamma v_{u-1}^{(i)}$, ..., $\Gamma v_1^{(i)}$) and ${}^tP$, respectively. Similarly, for BFN-(SP)^{u}S, the linear trails can be treated as the differential trails by replacing ($\Delta x_1^{(i)}$, $\Delta x_2^{(i)}$,..., $\Delta x_{u+1}^{(i)}$), ($\Delta y_1^{(i)}$, $\Delta y_2^{(i)}$,..., $\Delta y_{u+1}^{(i)}$) and P by ($\Gamma y_{u+1}^{(i)}$, $\Gamma y_u^{(i)}$,..., $\Gamma y_1^{(i)}$), ($\Gamma x_{u+1}^{(i)}$, $\Gamma x_u^{(i)}$,..., $\Gamma x_1^{(i)}$) and ${}^tP$, respectively. Therefore, since the constraints for differential and linear trails for the BFNs are the same, the minimum numbers of differentially and linearly active S-boxes can be derived simultaneously. The above discussions yield the following theorem.

Theorem 8. *For BFN-(SP)^u and BFN-(SP)^{u}S, assuming that both S-box layer and linear diffusion layer are bijective, the lower bounds on the number of differentially active S-boxes derived from the property of the linear diffusion layer hold also for the number of linearly active S-boxes by changing the linear diffusion layer to the transposed one.*

In the sequel, we only discuss the minimum numbers of differentially active S-boxes for simplicity, keeping in mind, however, that the minimum numbers of linearly active S-boxes can be derived in the same way.

7.4 Bounds for Active Functions

In this section, we give proofs for lower bounds on the minimum number of differentially active S-boxes for BFN-(SP)$^{2t+1}$, -(SP)^{2t}, -(SP)$^{2t-1}$S and -(SP)^{2t}S. These results are summarized in Table 7.1.

To prove those bounds, we utilize the following property and lemmata for BFNs consisting of bijective F-functions.

Property 15. *For each nonzero input difference, any two and three consecutive rounds of BFN consisting of bijective F-functions have at least one and two active functions, respectively.*

Proof. If two consecutive F-functions of the i-th and $(i+1)$-th rounds are both non-active, i.e., $\Delta X_L^{(i)}$ and $\Delta X_L^{(i+1)}$ are zero, the input difference $\Delta X_L^{(i)}$ and $\Delta X_U^{(i)} (= \Delta X_L^{(i+1)}$, since the output difference of the i-th round F-function is zero) are zero. Since this contradicts the assumption, at least one of two F-functions is active. From this, each of two consecutive rounds starting from the $(i-1)$-th round and the i-th round has at least one active F-function, which is an F-function whose input difference is nonzero. Obviously, if the i-th round F-function is non-active, three consecutive rounds starting from the $(i-1)$-th round have at least two active F-functions. If the i-th round F-function is active, $\Delta X_L^{(i-1)} (= \Delta X_U^{(i)})$ and $\Delta X_L^{(i+1)}$ cannot be zero simultaneously since the output difference of the i-th round F-function is nonzero. Therefore, there exist at least two active F-functions in three consecutive rounds. □

Meanwhile, the numbers of differentially active S-boxes for each differentially active F-function, which is an F-function whose input difference is nonzero, are lower-bounded by the following lemmata. Recall that $\mathcal{B}$ denotes the branch number of the linear layer.

Lemma 11 (**active S-boxes for 1-round BFN-(SP)^u**). *For BFN-(SP)^u, if $dw^{(i)}$ is not zero, $dw^{(i)} \geq \lfloor u/2 \rfloor \mathcal{B} + (u \mod 2)$.*

Proof. If an input difference of two consecutive SP-functions is not zero, there exist at least $\mathcal{B}$ active S-boxes, e.g., $dw_1^{(i)} + dw_2^{(i)} \geq \mathcal{B}$. Since BFN-(SP)^u has $\lfloor u/2 \rfloor$ independent two consecutive SP-functions and $(u \mod 2)$ SP-functions, it has at least $\lfloor u/2 \rfloor \mathcal{B} + (u \mod 2)$ active S-boxes when the input difference is not zero. □

Similarly to Lemma 11, one derives the following lemma.

Lemma 12 (**active S-boxes for 1-round BFN-(SP)^{u}S**). *For BFN-(SP)^{u}S, if $dw^{(i)}$ is not zero, $dw^{(i)} \geq \lceil u/2 \rceil \mathcal{B} + ((u+1) \mod 2)$.*

These lemmata show that the number of active S-boxes can be derived from the number of S-box layers when we treat only one active F-function. However, when we consider some consecutive rounds, the number of active S-boxes does not depend only on the number of S-box layers.

Starting from here, we treat four cases of the F-function construction separately: $(\mathrm{SP})^{2t+1}$, $(\mathrm{SP})^{2t}$, $(\mathrm{SP})^{2t-1}\mathrm{S}$, and $(\mathrm{SP})^{2t}\mathrm{S}$, as those exhibit essential differences.

7.4.1 Differentially Active S-Boxes in BFN-$(\mathrm{SP})^{2t+1}$

For BFN-$(\mathrm{SP})^{2t+1}$, which consists of odd number of SP-layers, the proofs for the lower bounds are the most complicated among other BFNs, since the number of differentially active S-boxes cannot be directly obtained from the number of differentially active F-functions. We find tight lower bounds on the minimum number of differentially active S-boxes by carefully observing two cases separately: $t = 0$ and other cases.

For BFN-$(\mathrm{SP})^{2t+1}$, Lemma 11 directly translates to the following corollary.

Table 7.1: Summary of our results, where $\mathcal{B}$ is the branch number of the diffusion matrix or its transpose, $\mathcal{E}_m = \lim_{r\to\infty} A_{m,r}/S_{m,r}$, and $\mathcal{E} = \lim_{m\to\infty} E_m$.

structure of F	$(\mathrm{SP})^{2t}$	$(\mathrm{SP})^{2t-1}\mathrm{S}$	$(\mathrm{SP})^{2t+1}$, $t=0$
proven tight bounds (min. # of active S-boxes / # of rounds)	$2t\mathcal{B}R$ / $3R$ $2t\mathcal{B}R$ / $(3R+1)$ $(2t\mathcal{B}R+t\mathcal{B})$ / $(3R+2)$ (Th. 11), (Th. 12)		$((\mathcal{B}+1)R-1)$ / $4R$ $(\mathcal{B}+1)R$ / $(4R+1)$ $((\mathcal{B}+1)R+1)$ / $(4R+2)$ $((\mathcal{B}+1)R+2)$ / $(4R+3)$ (Th. 9)
# of S-boxes in 1-round	$2mt$	$2mt$	m
$\mathcal{E}_m$	$2t\mathcal{B}/6mt$		$(\mathcal{B}+1)/4m$
$\mathcal{E}$ $(\mathcal{B}=m+1)$	$1/3$		$1/4$

structure of F	$(\mathrm{SP})^{2t+1}$, $t>0$	$(\mathrm{SP})^{2t}\mathrm{S}$
proven tight bounds (min. # of active S-boxes / # of rounds)	$((2t+1)\mathcal{B}R-\mathcal{B}+2)$ / $3R$ $(2t+1)\mathcal{B}R$ / $(3R+1)$ $((2t+1)\mathcal{B}R+t\mathcal{B}+1)/(3R+2)$ (Th. 10)	$2(t\mathcal{B}+1)R$ / $3R$ $2(t\mathcal{B}+1)R$ / $(3R+1)$ $(2(t\mathcal{B}+1)R+t\mathcal{B}+1)/(3R+2)$ (Th. 13)
# of S-boxes in 1-round	$(2t+1)m$	$(2t+1)m$
$\mathcal{E}_m$	$(2t+1)\mathcal{B}/3(2t+1)m$	$2(t\mathcal{B}+1)/3(2t+1)m$
$\mathcal{E}$ $(\mathcal{B}=m+1)$	$2t/3(2t+1)$	$2t/3(2t+1)$

Corollary 1. *For BFN-(SP)$^{2t+1}$, if $dw^{(i)}$ is not zero, $dw^{(i)} \geq t\mathcal{B}+1$.*

Property 15 and Corollary 1 directly show that any three consecutive rounds of BFN-$(\mathrm{SP})^{2t+1}$ have at least $2(t\mathcal{B}+1)$ active S-boxes. However, when the center of the F-function in the three consecutive rounds is active, there exist more active S-boxes as follows.

Lemma 13. *For BFN-(SP)$^{2t+1}$, if $dw^{(i)}$ is not zero, $dw^{(i-1)}+dw^{(i)}+dw^{(i+1)} \geq (2t+1)\mathcal{B}$.*

Proof. From the definition, $\Delta x_1^{(i-1)} \oplus \Delta x_1^{(i+1)} = M(\Delta y_{2t+1}^{(i)})$. If $dw^{(i)}$ is not zero, then $\Delta y_{2t+1}^{(i)}$ is not zero due to the invertibility. Since $\Delta y_{2t+1}^{(i)}$ is not zero, $w_n(\Delta x_1^{(i-1)}) + w_n(\Delta x_1^{(i+1)}) + w_n(\Delta y_{2t+1}^{(i)}) \geq \mathcal{B}$, i.e., $dw_1^{(i-1)} + dw_{2t+1}^{(i)} + dw_1^{(i+1)} \geq \mathcal{B}$. Also, if $\Delta y_{2t+1}^{(i)}$ is not zero, $\Delta x_1^{(i-1)}$ and $\Delta x_1^{(i+1)}$ cannot be zero simultaneously. Thus $dw_1^{(i-1)} + ... + dw_{2t}^{(i-1)} \geq t\mathcal{B}$ or $dw_1^{(i+1)} + ... + dw_{2t}^{(i+1)} \geq t\mathcal{B}$. Therefore $\Sigma_{j=1}^{2t+1}(dw_j^{(i-1)} + dw_j^{(i)} + dw_j^{(i+1)}) \geq (2t+1)\mathcal{B}$. □

The lower bounds on the minimum number of active S-boxes in any consecutive rounds of BFN-$(\mathrm{SP})^{2t+1}$ are directly derived by the lemmata above. First, we prove the bounds on $\mathcal{D}(r)$, $r \leq 4$ by Lemma 14, then show the bounds on $\mathcal{D}(r)$, $r > 4$ by Lemma 15.

Lemma 14. *For BFN-(SP)$^{2t+1}$, $\mathcal{D}(1) = 0$, $\mathcal{D}(2) = t\mathcal{B}+1$, $\mathcal{D}(3) = 2(t\mathcal{B}+1)$, and $\mathcal{D}(4) = (2t+1)\mathcal{B}$.*

Proof. Since any two consecutive rounds have at least one active F-function, $\mathcal{D}(2) = t\mathcal{B}+1$ from Corollary 1. We consider $dw^{(i-1)}$, $dw^{(i)}$ and $dw^{(i+1)}$. If $dw^{(i)}$ is not zero, then $dw^{(i-1)} + dw^{(i)} + dw^{(i+1)} \geq (2t+1)\mathcal{B}$. If $dw^{(i)}$ is zero, then both $dw^{(i-1)}$ and $dw^{(i+1)}$ are not zero from Property 15. In that case, $dw^{(i-1)} + dw^{(i)} + dw^{(i+1)} \geq 2(t\mathcal{B}+1)$ from Corollary 1. Since $\mathcal{B} \geq 2$ from the invertibility and $(2t+1)\mathcal{B} \geq 2(t\mathcal{B}+1)$, we obtain $\mathcal{D}(3) = 2(t\mathcal{B}+1)$. We consider $dw^{(i-1)}$, $dw^{(i)}$, $dw^{(i+1)}$ and $dw^{(i+2)}$. If $dw^{(i)}$ is not zero, $dw^{(i-1)} + dw^{(i)} + dw^{(i+1)} \geq (2t+1)\mathcal{B}$ from Lemma 13. If $dw^{(i)}$ is zero, then $dw^{(i+1)}$ is not zero due to the invertibility. Then $dw^{(i)} + dw^{(i+1)} + dw^{(i+2)} \geq (2t+1)\mathcal{B}$. Thus, $\mathcal{D}(4) = (2t+1)\mathcal{B}$. □

The bounds on $\mathcal{D}(r)$, $r > 4$, are given as inductive forms.

Lemma 15. *Let $r > 4$, $\mathcal{D}(r) = \min(\mathcal{D}(r-3) + (2t+1)\mathcal{B}, \mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1)$ for BFN-(SP)$^{2t+1}$.*

Proof. We consider active S-boxes in r consecutive rounds starting from round $i+1$, i.e., $dw^{(i+1)}, ..., dw^{(i+r)}$. If $dw^{(i+r-1)}$ is not zero, then $dw^{(i+r-2)} + dw^{(i+r-1)} + dw^{(i+r)} \geq (2t+1)\mathcal{B}$. Also, $dw^{(i+1)} + ... + dw^{(i+r-3)} \geq \mathcal{D}(r-3)$ from the definition. Therefore, $dw^{(i+1)} + ... + dw^{(i+r)} \geq \mathcal{D}(r-3) + (2t+1)\mathcal{B}$ when $dw^{(i+r-1)}$ is not zero. If $dw^{(i+r-1)}$ is zero, then both $dw^{(i+r-2)}$ and $dw^{(i+r)}$ are nonzero. $dw^{(i+r-3)} + dw^{(i+r-2)} + dw^{(i+r-1)} \geq (2t+1)\mathcal{B}$ and $dw^{(i+r)} \geq t\mathcal{B}+1$ from Corollary 1. Also, $dw^{(i+1)} + ... + dw^{(i+r-4)} \geq \mathcal{D}(r-4)$. Therefore, $dw^{(i+1)} + ... + dw^{(i+r)} \geq \mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1$ when $dw^{(i+r-1)}$ is zero. Combining both results, we obtain $\mathcal{D}(r) = \min(\mathcal{D}(r-3) + (2t+1)\mathcal{B}, \mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1)$ when $r > 4$. □

Now we have the lower bounds in any consecutive rounds of BFN-(SP)$^{2t+1}$. However, it is hard to compare its efficiency with other constructions, since the bounds are proven as inductive forms. In order to obtain more accurate bounds, we consider two cases. We start with the special case of $t = 0$.

Theorem 9 (active S-boxes for BFN-(SP)$^{2t+1}, t = 0$). *For any nonzero input difference (nonzero input mask), every $4R$, $4R+1$, $4R+2$, $4R+3$ rounds of BFN ($R \geq 1$) with an SP F-function provide at least $(\mathcal{B}+1)R-1$, $(\mathcal{B}+1)R$, $(\mathcal{B}+1)R+1$, $(\mathcal{B}+1)R+2$ differentially (linearly) active S-boxes, respectively, assuming $\mathcal{B} > 2$, where $\mathcal{B}$ is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

Proof. If $\mathcal{D}(r-3) - \mathcal{D}(r-4) \geq 1$, $\mathcal{D}(r) = \mathcal{D}(r-4) + \mathcal{B} + 1$ from Lemma 15. Otherwise $\mathcal{D}(r) = \mathcal{D}(r-3) + \mathcal{B}$. Clearly, $\mathcal{D}(r-3) - \mathcal{D}(r-4) = 1$ when $r = 5$ and 6, and $\mathcal{D}(r-3) - \mathcal{D}(r-4) = \mathcal{B} - 2$ when $r = 7$. Since $\mathcal{B} > 2$ from the assumption, $\mathcal{D}(r-3) - \mathcal{D}(r-4) \geq 1$ when $r = 7$. Similarly, $\mathcal{D}(r-3) - \mathcal{D}(r-4) = \mathcal{D}(5) - \mathcal{D}(4) = (\mathcal{B}+1) - (\mathcal{B}) = 1$ when $r = 8$. Since $\mathcal{D}(r-3) - \mathcal{D}(r-4) \geq 1$ for $r = 5, 6, 7$ and 8, $\mathcal{D}(r-3) - \mathcal{D}(r-4) \geq 1$ when $r \geq 5$. Thus $\mathcal{D}(r) = \mathcal{D}(r-4) + \mathcal{B} + 1$ when $r \geq 5$. Then $\mathcal{D}(r) = \mathcal{D}(r-4) + \mathcal{B} + 1 = \mathcal{D}(r-8) + 2(\mathcal{B}+1) = \cdots = \mathcal{D}(r-4u) + (\mathcal{B}+1)u$. Therefore $\mathcal{D}(4R+1) = \mathcal{D}(4R-3) + \mathcal{B} + 1 = \mathcal{D}(4R-7) + 2(\mathcal{B}+1) = \cdots = \mathcal{D}(1) + (\mathcal{B}+1)R = (\mathcal{B}+1)R$. Similarly, $\mathcal{D}(4R+2) = \mathcal{D}(2) + (\mathcal{B}+1)R = (\mathcal{B}+1)R+1$, $\mathcal{D}(4R+3) = \mathcal{D}(3) + (\mathcal{B}+1)R = (\mathcal{B}+1)R+2$, $\mathcal{D}(4R) = \mathcal{D}(4) + (R-1)(\mathcal{B}+1) = (\mathcal{B}+1)R - 1$. □

Note that Theorem 9 was conjectured in [Shi01]. For all other integers $t > 0$, the bounds are stated as follows.

Theorem 10 (active S-boxes for BFN-(SP)$^{2t+1}, t > 0$). *For any nonzero input difference (nonzero input mask), every $3R$, $3R+1$, $3R+2$ rounds of BFN ($R \geq 1$) with $(2t+1)$ consecutive SP-layers in the F-function ($t > 0$) provide at least $(2t+1)\mathcal{B}R - \mathcal{B} + 2$, $(2t+1)\mathcal{B}R$, $(2t+1)\mathcal{B}R + t\mathcal{B} + 1$ differentially (linearly) active S-boxes, respectively, where $\mathcal{B}$ is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

Proof. If $\mathcal{D}(r-3) - \mathcal{D}(r-4) \leq t\mathcal{B} + 1$, $\mathcal{D}(r) = \mathcal{D}(r-3) + (2t+1)\mathcal{B}$ from Lemma 15. Otherwise $\mathcal{D}(r) = \mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1$. From Lemma 14, $\mathcal{D}(r-3) - \mathcal{D}(r-4) = t\mathcal{B} + 1$ when $r = 5$ and 6, and $\mathcal{D}(r-3) - \mathcal{D}(r-4) = \mathcal{B} - 2$ when $r = 7$. Since $t > 0$,

$\mathcal{B} - 2 < t\mathcal{B} + 1$. Thus $\mathcal{D}(r) = \mathcal{D}(r-3) + (2t+1)\mathcal{B}$ when $r \geq 5$. Then $\mathcal{D}(r) = \mathcal{D}(r-3) + (2t+1)\mathcal{B} = \mathcal{D}(r-6) + 2(2t+1)\mathcal{B} = \cdots = \mathcal{D}(r-3u) + (2t+1)\mathcal{B}u$. Therefore $\mathcal{D}(3R+1) = \mathcal{D}(3R-2) + (2t+1)\mathcal{B} = \cdots = \mathcal{D}(1) + (2t+1)\mathcal{B}R = (2t+1)\mathcal{B}R$. Similarly, $\mathcal{D}(3R+2) = \mathcal{D}(2) + (2t+1)\mathcal{B}R = (2t+1)\mathcal{B}R + t\mathcal{B} + 1$, $\mathcal{D}(3R) = \mathcal{D}(3) + (2t+1)(R-1)\mathcal{B} = (2t+1)\mathcal{B}R - \mathcal{B} + 2$. □

Now we have comparable bounds for every four rounds of BFN-$(\mathrm{SP})^{2t+1}$. For the case of $t > 0$, $(\mathcal{D}(r-3) + (2t+1)\mathcal{B})$ is always less than or equal to $(\mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1)$. On the other hands, for the case of $t = 0$, $(\mathcal{D}(r-4) + \mathcal{B} + 1)$ is less than or equal to $(\mathcal{D}(r-3) + \mathcal{B})$ when $\mathcal{B} > 2$ and $r = 4s + 3 (s > 0)$ (e.g., $r = 7, 11, 15, ...$). Thus, the bounds for the case $t = 0$ and $t > 0$ are slightly different and those are separately proven. The tightness of these bounds is proven in Section 7.5.

7.4.2 Differentially Active S-Boxes in BFN-$(\mathrm{SP})^{2t}$

For BFN-$(\mathrm{SP})^{2t}$, which comprises even number of SP-layers, the minimum number of differentially active S-boxes is straightforwardly proven by observing the number of differentially active F-functions.

Lemma 11 yields the following corollary.

Corollary 2. *For BFN-$(SP)^{2t}$, if $dw^{(i)}$ is not zero, $dw^{(i)} \geq t\mathcal{B}$.*

This corollary allows us to prove the following theorem.

Theorem 11 (**active S-boxes for BFN-$(\mathrm{SP})^{2t}$**). *For any nonzero input difference (nonzero input mask), every $3R$, $3R+1$, $3R+2$ rounds of BFN ($R \geq 1$) with $2t$ consecutive SP layers in the F-function provide at least $2t\mathcal{B}R$, $2t\mathcal{B}R$, $2t\mathcal{B}R + t\mathcal{B}$ differentially (linearly) active S-boxes, respectively, where $\mathcal{B}$ is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

Proof. We consider $dw^{(i-1)}, dw^{(i)}$ and $dw^{(i+1)}$. If $dw^{(i)}$ is zero, then both $dw^{(i-1)}$ and $dw^{(i+1)}$ are not zero due to the invertibility. Thus there exist at least $2t\mathcal{B}$ active S-boxes from Corollary 2. If $dw^{(i)}$ is not zero, then $dw^{(i-1)}$ and $dw^{(i+1)}$ cannot be zero simultaneously. Therefore there exist at least $2t\mathcal{B}$ active S-boxes from Corollary 2. Since two consecutive rounds have at least $t\mathcal{B}$ active S-boxes, $3R + 2$ consecutive rounds have at least $2t\mathcal{B}R + t\mathcal{B}$ active S-boxes. □

Unlike the case of BFN-$(\mathrm{SP})^{2t+1}$, the lower bounds for BFN-$(\mathrm{SP})^{2t}$ are easily proven. In the other words, the minimum number of differentially active S-boxes for BFN-$(\mathrm{SP})^{2t}$ corresponds to the minimum number of differential active F-functions times $t\mathcal{B}$.

7.4.3 Differentially Active S-Boxes in BFN-$(\mathrm{SP})^{2t-1}\mathrm{S}$

Since the number of S-box layers is the same in BFN-$(\mathrm{SP})^{2t-1}$S, similarly to the bounds for BFN-$(\mathrm{SP})^{2t}$, one derives the following theorem.

Theorem 12 (**active S-boxes for BFN-$(\mathrm{SP})^{2t-1}\mathrm{S}$**). *For any nonzero input difference (nonzero input mask), every $3R$, $3R+1$, $3R+2$ rounds of BFN ($R \geq 1$) with $(2t-1)$ consecutive SP-layers followed by an S-box layer in the F-function provide at least $2t\mathcal{B}R$,*

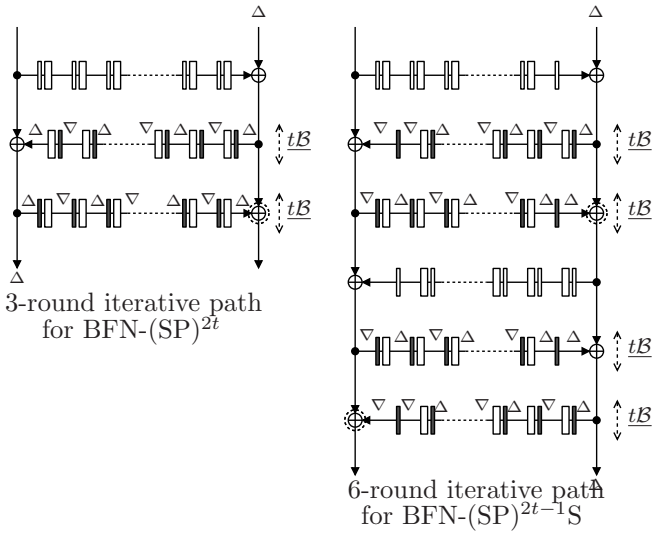

Figure 7.4: Truncated differential trails of BFN-(SP)^{2t} (left: 3-round iterative trail) and BFN-(SP)$^{2t-1}$S (right: 6-round iterative trail) attaining the lower bounds of Theorems 11 and 12.

$2t\mathcal{B}R$, $2t\mathcal{B}R + t\mathcal{B}$ differentially (linearly) active S-boxes, where $\mathcal{B}$ is the branch number of the diffusion matrix (of the transposed diffusion matrix).

The obtained bounds for BFN-(SP)^{2t}S seem almost same as the bounds for BFN-(SP)^{2t}. However, BFN-(SP)^{2t} has one more P-layer than BFN-(SP)$^{2t-1}$S has when the parameter t is the same. This implies that the last P-layer of BFN-(SP)^{2t} does not improve the security in terms of the number of differentially active S-boxes.

7.4.4 Differentially Active S-Boxes in BFN-(SP)^{2t}S

Similarly to BFN-(SP)$^{2t+1}$, BFN-(SP)^{2t}S has odd number of S-layers. However, lack of the last P-layer allows us to prove the bounds for BFN-(SP)^{2t}S easily.

Property 15 and Lemma 12 yield the following theorem.

Theorem 13 (active S-boxes for BFN-(SP)^{2t}S). *For any nonzero input difference (nonzero input mask), every $3R$, $3R+1$, $3R+2$ rounds of BFN ($R \geq 1$) with $2t$ consecutive SP-layers followed by an S-box layer in the F-function provide at least $2(t\mathcal{B}+1)R$, $2(t\mathcal{B}+1)R$, $(2(t\mathcal{B}+1)R+(t\mathcal{B}+1))$ differentially (linearly) active S-boxes, where $\mathcal{B}$ is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

The proof for BFN-(SP)^{2t}S is similar to the proofs for BFN-(SP)^{2t} and BFN-(SP)$^{2t-1}$S. In other words, for BFN-(SP)^{2t}S, the minimum number of active S-boxes can be proven by studying the number of active F-functions. However, the proven bounds are not same as the bounds for BFN-(SP)^{2t} and BFN-(SP)$^{2t-1}$S, since the number of S-layers is different. In the following sections, we discuss tightness of the bounds proven in this section and their optimality.

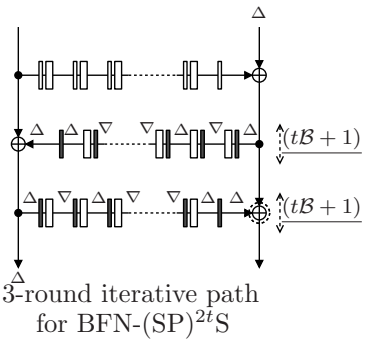

Figure 7.5: Truncated differential trails of BFN-(SP)^{2t}S (3-round iterative trail) attaining the lower bounds of Theorem 13.

7.5 Tightness of Bounds

To demonstrate the tightness of the lower bounds, we provide trails that actually attain those proven bounds when the matrices used in the BFNs are MDS. These trails are given in Figs. 7.4 to 7.7 for all the BFN constructions in question. Note that a similar observation for BFN-SP with $m = 8$ was given in Appendix A of [SS04].

In the figures, Δ and ∇ denote S-box truncated difference 100...00 (only the first S-box active out of m) and 111...11 (all m S-boxes active), respectively. Thin boxes and thick boxes denote S-box layers (S-layers) and linear layers (P-layers), respectively. XORs with difference cancellation are marked with dashed circles. Differentially active S-box layers are denoted by grey. The underlined numbers denote the minimum numbers of active S-boxes in the area indicated by a dashed line.

From the discussions in Section 7.3, the following observations are directly applicable to the case of the linear cryptanalysis.

7.5.1 BFN-(SP)^{2t}

The left side of Fig. 7.4 shows a 3-round iterative path that maps $(0, \Delta)$ to $(0, \Delta)$ for BFN-(SP)^{2t}. In other words, the i-th round input difference $(\Delta X_L^{(i)}, \Delta X_U^{(i)}) = (0, \Delta)$ and the $(i+3)$-th round input difference $(\Delta X_L^{(i+3)}, \Delta X_U^{(i+3)}) = (0, \Delta)$. Note that, since we use an untwisted form in Fig. 7.4, an output difference looks reverse in the case of odd number of rounds. The numbers of active S-boxes provided by this figure correspond to the bounds proven in Theorem 11. For instance, the numbers of active S-boxes for 3, 4, 5 and 6 rounds given by the figure are $2t\mathcal{B}$, $2t\mathcal{B}$, $3t\mathcal{B}$ and $4t\mathcal{B}$, respectively, which correspond to the proven bounds. Since the path is 3-round iterative, it shows that the proven bounds are tight.

7.5.2 BFN-(SP)$^{2t-1}$S and BFN-(SP)^{2t}S

The right side of Fig. 7.4 shows a 6-round iterative path for BFN-(SP)$^{2t-1}$S that maps $(0, \Delta)$ to $(0, \Delta)$. There does not exist a simple 3-round iterative path, since the output difference of the F-function will be $\nabla(\Delta)$ when the input difference of F-function is $\Delta(\nabla)$.

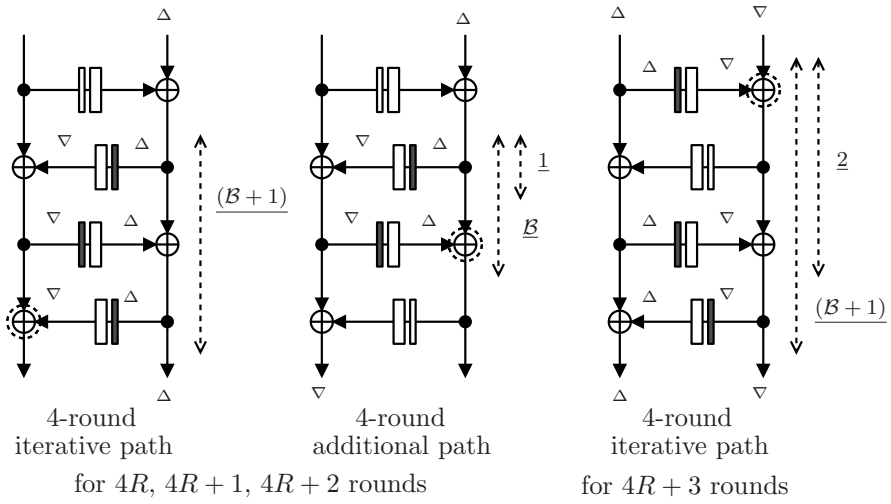

Figure 7.6: Truncated differential trails of BFN-SP attaining the lower bounds of Theorem 9.

However, those become iterative when considered over 6 rounds. The paths shown in the figure provide $2t\mathcal{B}$ active S-boxes for 3 rounds and prove the tightness of the bounds proven in Theorem 12. Figure 7.5 shows a 3-round iterative path for BFN-$(\mathrm{SP})^{2t}$S that attains the lower bounds proven in Theorem 13.

7.5.3 BFN-SP

The paths of Fig. 7.6 for BFN-SP consist of iterative paths and an additional path. In the case of $(4R + 3)$ rounds, the tightness is easily proven by the right side of Fig. 7.6. In the other cases ($4R$, $4R + 1$ and $4R + 2$ rounds), paths consist of some consecutive 4-round iterative paths on the left and one 4-round additional path in the center of Fig. 7.6. Each path for $4R$ rounds consists of $(R - 1)$ consecutive 4-round iterative paths and one 4-round additional path. Also paths for $4R + 1$ and $4R + 2$ rounds consist of R consecutive 4-round iterative paths and one 4-round additional path. For example, a path for 12 rounds of BFN-SP consists of two consecutive 4-round iterative paths followed by one 4-round additional path. Similarly, a path for 13 rounds consists of three 4-round iterative paths (12 rounds) followed by the first one round of the 4-round additional path (1 round).

7.5.4 BFN-$(\mathrm{SP})^{2t+1}$, $t > 0$

Figure 7.7 shows a 6-round iterative path that attains the bounds proven in Theorem 10. The path starting from the i-th round shows the tightness for $3R + 1$ and $3R + 2$ rounds. The path starting from the $(i + 2)$-th round shows the tightness for $3R$ rounds.

7.6 Optimality

In this section, it is proven that BFN-SPS and BFN-SPSP are the most efficient with respect to the efficiency metric $\mathcal{E}_m$ of Definition 13. Recall that $\mathcal{E}_m$ shows the ratio between active S-boxes and all S-boxes when the number of rounds is sufficiently large. Table 7.2 contains the computation of $\mathcal{E}_m$ for the different BFNs in question. The optimality result is formulated as follows.

Theorem 14. *When instantiated with MDS matrices for $m \geq 2$, BFN-$(SP)^{2t}$ and BFN-$(SP)^{2t-1}S$ provide a higher or equal proportion of active S-boxes than BFN-SP, BFN-$(SP)^{2t+1}$ and BFN-$(SP)^{2t}S$ for any number t of layers. Thus, BFN-SPSP and BFN-SPS are optimal with respect to $\mathcal{E}_m$.*

Proof. We compute the values of $\mathcal{E}_m$ for all BFN constructions with MDS matrices in Table 7.2 and compare $\mathcal{E}_m = \frac{m+1}{3m}$ for BFN-$(SP)^{2t}$ and BFN-$(SP)^{2t-1}S$ to $\mathcal{E}_m$ for

- **BFN-$(SP)^{2t+1}$.** From Table 7.2, one immediately observes that $\frac{m+1}{3m}$ is no lower than $\mathcal{E}_m$ for BFN-$(SP)^{2t+1}$.
- **BFN-SP.** For $m \geq 2$, the difference $\frac{m+1}{3m} - \frac{m+2}{4m} = \frac{m-2}{12m} \geq 0$ and $\mathcal{E}_m$ for BFN-SP is no higher than $\frac{m+1}{3m}$.
- **BFN-$(SP)^{2t}$S.** In this case, one has to analyze $\frac{2t(m+1)+2}{3(2t+1)m}$ as a function of t. After taking the value of 0 for $t = -\frac{1}{m+1}$, it grows monotonously for all $t > 0$ and attains its maximum at the infinity. Since

$$\lim_{t\to\infty} \frac{2t(m+1)+2}{3(2t+1)m} = \frac{m+1}{3m},$$

  $\mathcal{E}_m$ for BFN-$(SP)^{2t}$S is no higher than $\frac{m+1}{3m}$.

Thus, $\mathcal{E}_m$ for BFN-$(SP)^{2t}$ and BFN-$(SP)^{2t-1}$S is no lower than that for BFN-$(SP)^{2t+1}$, BFN-SP, and BFN-$(SP)^{2t}$S, which yields the first claim of the theorem. The second claim follows from choosing $t = 1$. □

7.7 Conclusions

In this chapter, we considered a wide class of balanced Feistel networks with any number of interleaved S-box layers and linear diffusion layers in their F-function. In this class, we demonstrated that SPS and SPSP F-functions are arguably optimal with respect to the relative number of active S-boxes provided. Our results indicate that one SP-layer in the F-function is not enough to attain optimality, whereas taking more than two S-box layers does not increase the efficiency either. The optimality is shown with respect to the security of a cipher towards differential and linear cryptanalysis.

As nearly any SPN-based block cipher, BFNs with SP-type F-functions exhibit the differential effect – many differential trails contributing to the same differential. Having SPS or SPSP constructions as F-functions – as in the optimal constructions of this chapter

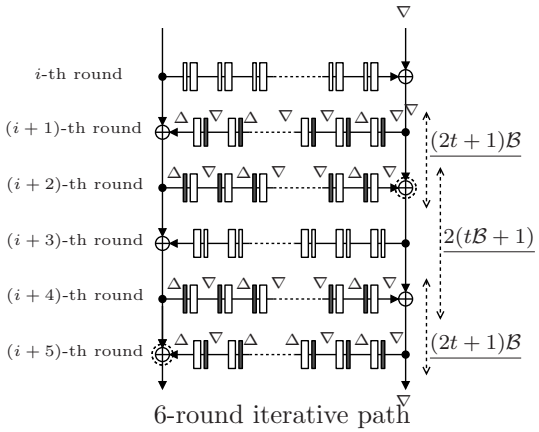

Figure 7.7: Truncated differential trails of BFN-$(\mathrm{SP})^{2t+1}$, $t > 0$ (6-round iterative trail) attaining the lower bounds of Theorem 10.

– simplifies the consideration of upper bounds on the differential probability over several rounds. The work [AO97] proves that the maximum average differential probability over 3 rounds for a BFN with bijective F-functions is upper-bounded by π^2, where π is the maximum differential probability of the F-function. At the same time, the maximum differential probability of an SPS or SPSP construction with MDS diffusion is known to be upper-bounded by p^m, where p is the maximum differential probability of the underlying S-box [KHL+01]. This provides an upper bound of p^{2m} on the average differential probability over 3 rounds of BFN-SPS and BFN-SPSP. Similar considerations apply to the linear probability. However, capturing the differential or linear hull effect for an arbitrary number of rounds and incorporating it into the efficiency metric appears to be a challenging task.

Besides BFNs, generalized Feistel networks (GFNs) are often used in the design of block ciphers. Both CLEFIA [SSA+07] and PICCOLO [SIH+11] follow this design approach with SP-type F-functions. We conjecture that our optimality result also applies to any GFN under the definition of [BS13]. In other words, our conjecture is that the instantiation of the F-function with SPS and SPSP will be optimal with respect to the relative number of active S-boxes. We leave this as an important open problem.

Table 7.2: $\mathcal{E}_m$ for BFNs with SP-type functions and MDS matrices

Construction	$A_{r,m}$	$S_{r,m}$	$\mathcal{E}_m = \lim_{r\to\infty} \frac{A_{r,m}}{S_{r,m}}$
BFN-$(\mathrm{SP})^{2t}$ BFN-$(\mathrm{SP})^{2t-1}$S	$A_{3R,m} = 2t(m+1)R$ $A_{3R+1,m} = 2t(m+1)R$ $A_{3R+2,m} = (2tR+t)(m+1)$	$2tmr$	$\frac{m+1}{3m}$
BFN-$(\mathrm{SP})^{2t+1}$	$A_{3R,m} = ((2t+1)R-1)(m+1)+2$ $A_{3R+1,m} = (2t+1)(m+1)R$ $A_{3R+2,m} = ((2t+1)R+t)(m+1)+1$	$(2t+1)mr$	$\frac{m+1}{3m}$
BFN-SP	$A_{4R,m} = (m+2)R-1$ $A_{4R+1,m} = (m+2)R$ $A_{4R+2,m} = (m+2)R+1$ $A_{4R+3,m} = (m+2)R+2$	mr	$\frac{m+2}{4m}$
BFN-$(\mathrm{SP})^{2t}$S	$A_{3R,m} = 2(t(m+1)+1)R$ $A_{3R+1,m} = 2(t(m+1)+1)R$ $A_{3R+2,m} = (2R+1)(t(m+1)+1)$	$(2t+1)mr$	$\frac{2t(m+1)+2}{3(2t+1)m}$

Chapter 8

Optimal Round Diffusion of Generalized Feistel Networks

8.1 Introduction

8.1.1 Motivation and Previous Work

As one of the diffusion properties, the diffusion round (DRmax) was defined in [SM10]. This is defined as the minimal number of rounds such that every sub-block of the ciphertext depends on every sub-block of the plaintext. While DRmax(π) is a simple property that can be efficiently calculated from the given round permutation π, it has a strong relevance to immunity against impossible differential [BBS99] and saturation attacks [DKR97], which are powerful attacks especially for GFN.

In [SM10], Suzaki and Minematsu showed that DRmax of type-II GFNs can be improved by using an appropriate round permutation instead of a cyclic shift for d-line GFN (denoted as GFN_d), where $d \geq 6$. Then, optimal, regarding DRmax, single even-odd round permutations (every even numbered input is permuted to an odd numbered output and vice versa by the pre-determined manner) for 6- to 16-line GFNs were shown by exhaustively searching all possible single even-odd round permutations. Lately, [CGT19, DFLM19] extend their ideas by thoroughly analyzing equivalent classes and improving the search algorithm, and show optimal single even-odd round permutations for 18- to 32- and 36-line GFNs.

The lower bounds on DRmax for GFN with even-odd permutations have been given by Fibonacci sequence in [SM10]. However, there still exist several gaps between the theoretical lower bounds and the known optimal results. For instance, the lower bounds on DRmax for GFN_{10} and GFN_{12} are 6 and 7, however, DRmax for them with the optimal single round permutation are 7 and 8, respectively. This indicates that, for some d, GFN_d with a single round permutation cannot reach the lower bounds on DRmax. However, it still has not been known whether there exist tight round permutations reaching the theoretical lower bounds. In this chapter, we tackle this problem.

Table 8.1: Lower bounds, known optimal results and our results on DRmax for GFN_d, where $d = 6, \ldots, 12$, π^{1RP}, π^{2RP} and π^{SD} denote the round permutation with single permutation, double permutation and sub-block dividing, respectively.

d	DRmax (Lower bounds)	DRmax(π^{1RP}) (Known optimal)	DRmax(π^{2RP}) (Section 8.4)	DRmax(π^{SD}) (Section 8.3)
6	5	5	5	$\underline{\mathbf{4}}$
8	6	6	6	$\underline{\mathbf{4}}$
10	6	7	**7**	$\underline{\mathbf{4}}$
12	7	8	$\underline{\mathbf{7}}$	$\underline{\mathbf{4}}$

8.1.2 Improving the Round Diffusion of GFN

In order to improve the diffusion round of GFN, we propose two techniques: one using a non sub-block wise permutation and the other one using sub-block wise permutations. We first propose a technique called sub-block dividing, which further divides each sub-block into $(d/2)$ smaller blocks. The sub-block dividing for GFN_4 was previously used in the round permutation of the block cipher Piccolo [SIH+11]. We generalize it to any $d \geq 4$ of GFN_d. This is an improvement using a non sub-block wise permutation.

In order to find tight sub-block wise round permutations, we expand the search space from single round permutations to multiple round permutations. The previous results [SM10, CGT19, DFLM19] focus on the case of single round permutations, and the use multiple round permutations in GFNs has not been addressed so far. We investigate the (im)possibilities of further improving diffusion of GFNs with multiple round permutations, especially we focus on the problem if the proposed construction can achieve the lower bounds on DRmax, which has not been known so far.

8.1.3 Contributions

We first generalize a round permutation with sub-block dividing to any $d \geq 4$ of GFN_d. Then, we prove that four rounds of GFN using round permutations with sub-block dividing always achieve nonlinearly full diffusion. Moreover, we show that a 10- and 12-line GFN alternately using two different round permutations (denoted as $\mathrm{GFN}_{10}^{\mathrm{2RP}}$ and $\mathrm{GFN}_{12}^{\mathrm{2RP}}$) partially and fully achieve the lower bounds on DRmax, respectively. This class of GFN has not been known so far. Our results imply the possibilities of improving the round diffusion of GFN by appropriately modifying those round permutations. See Table 8.1 for the summary of the lower bounds, known results, and our results.

8.2 Diffusion Round

This section provides definitions and a proposition used in this chapter. We focus on GFNs with even-odd round permutations defined in Section 3.1. In this chapter, we propose to alternately use two different round permutations π_0 and π_1. Those specific constructions treated in this chapter are depicted in Fig. 8.1. Each sub-block of the $(r+1)$-round input $x_i^{(r+1)}$ is computed from the r-round output without round permutation $y_i^{(r)}$

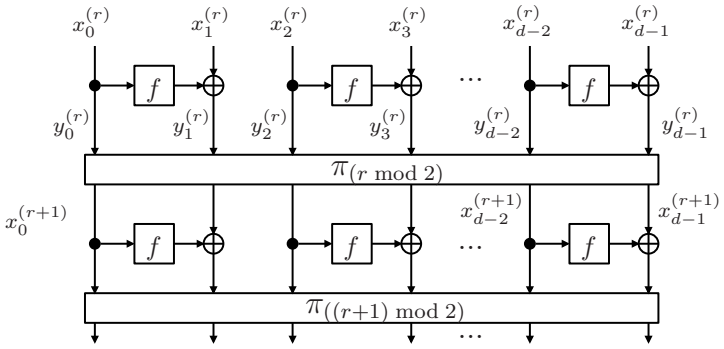

Figure 8.1: d-line GFN alternately using two different round permutations

and a round permutation π_0 or π_1 as follows:

$$x_i^{(r+1)} = y^{(r)}_{\pi_{(r \bmod 2)}(i)}, i \in \{0, \ldots, d-1\}\,.$$

The round permutations π_0 and π_1 can be divided into even-odd permutations p_0 and p_1, and odd-even permutations q_0 and q_1 as follows:

$$x_i^{(r+1)} = \begin{cases} y^{(r)}_{2p_{(r \bmod 2)}(i/2)+1} & \text{if } i \text{ is even}\,, \\ y^{(r)}_{2q_{(r \bmod 2)}((i-1)/2)} & \text{if } i \text{ is odd}\,. \end{cases}$$

That is, when r is even, $x_i^{(r+1)}$ is obtained as $y^{(r)}_{2p_0(i/2)+1}$ for $i = 0, 2, 4, \ldots, d-2$, and it is obtained as $y^{(r)}_{2q_0((i-1)/2)}$ for $i = 1, 3, 5, \ldots, d-1$. Similarly, we use p_1 and q_1 when r is odd, i.e., $x_i^{(r+1)}$ is $y^{(r)}_{2p_1(i/2)+1}$ for $i = 0, 2, 4, \ldots, d-2$, and it is $y^{(r)}_{q_1((i-1)/2)}$ for $i = 1, 3, 5, \ldots, d-1$.

If $\pi_0 \neq \pi_1$, we say that the d-line GFN alternately uses two different round permutations (denoted as $\mathrm{GFN}_d^{\mathrm{2RP}}$). Otherwise (i.e., $\pi_0 = \pi_1$), we say that the d-line GFN uses a single round permutation (denoted as $\mathrm{GFN}_d^{\mathrm{1RP}}$).

Proposition 11 (**Lower bounds on DRmax [SM10, CGT19, DFLM19]**). *Let $\mathcal{F}_i$ be the Fibonacci sequence, i.e. $\mathcal{F}_0 = 0, \mathcal{F}_1 = 1$, and $\mathcal{F}_i = \mathcal{F}_{i-1} + \mathcal{F}_{i-2}$ for $i \geq 2$. Then the lower bounds on DRmax of GFN_d using even-odd round permutations are given as $(i+1)$, where i is the smallest number satisfying $\mathcal{F}_i \geq d/2$.*

The proofs of Proposition 11 are given in [SM10, CGT19, DFLM19]. A difference in an odd numbered block is diffused to only one even numbered block in the next round. Similarly to this, a difference in an even numbered block is diffused to one even numbered block and one odd numbered block in the next round. Hence, if all odd numbered blocks in a certain round are affected by any input blocks, all output blocks in the next round are affected by any input blocks. If a round permutation works ideally, the number of odd numbered blocks affected is counted by $\mathcal{F}_i$. Therefore, the lower bounds on DRmax are given by Proposition 11.

For a given round permutation π, if $\mathrm{DRmax}(\pi)$ reaches the lower bound given in Proposition 11, we say that π is tight. Table 8.1 presents the lower bounds, the previously optimal results [SM10], and our results on DRmax of GFN_d, where $6 \leq d \leq 12$.

Since, in [SM10], the authors exhaustively searched over all the possible single round permutations for $6 \leq d \leq 16$, there do not exist tight permutations for $10 \leq d \leq 16$ when using a single round permutation. However, the problem of the existence of tight permutations for $10 \leq d \leq 16$ is still open.

8.3 Improving the Diffusion Round by Round Permutation with Sub-Block Dividing

In this section, we propose to use a round permutation with sub-block dividing to improve the diffusion round of GFN.

8.3.1 Sub-Block Dividing

The round permutation with sub-block dividing for GFN_4 was previously used in the round permutation of the block cipher Piccolo [SIH+11]. We generalize their technique to any $d \geq 4$ of GFN_d. Let $y_{i,j}^{(r)}$ and $x_{i,j}^{(r+1)}$ be $(d/2)$ partitions of $y_i^{(r)}$ and $x_i^{(r+1)}$, where $0 \leq i \leq (d-1)$ and $0 \leq j \leq (d/2-1)$. That is, we have $y_i^{(r)} = (y_{i,0}^{(r)}, \ldots, y_{i,d/2-1}^{(r)})$ and $x_i^{(r+1)} = (x_{i,0}^{(r+1)}, \ldots, x_{i,d/2-1}^{(r+1)})$. Then $x_i^{(r+1)}$ is calculated by the round permutation with sub-block dividing π^{SD} as follows:

$$x_{i,j}^{(r+1)} = \begin{cases} y_{((i+2j+1) \bmod d),j}^{(r)} & \text{if } i \text{ is even}, \\ y_{((d+i-2j-3) \bmod d),j}^{(r)} & \text{if } i \text{ is odd}. \end{cases}$$

$\mathrm{DRmax}(\pi^{\mathrm{SD}})$ of GFN_d is given as follows:

Theorem 15 (DRmax of $\pi^{\mathbf{SD}}$). *For any $d \geq 4$, the diffusion round of π^{SD} is always four, assuming that the underlying F-function is a sufficiently good nonlinear function.*

Proof. For any non-zero input difference, at least one of F-function inputs in the 2nd round has a non-zero difference. The output of the F-function having a non-zero input difference in the 2nd round has a non-zero difference due to the randomness of the F-function. Such non-zero output difference of the F-function propagates to all the even numbered sub-blocks of the 3rd round input by π^{SD}. This means that all the F-function inputs in the 3rd round have a non-zero difference.

Similarly to the 2nd round, all the outputs of the F-functions in the 3rd round have a non-zero difference, and those non-zero output differences propagate to all the even numbered sub-blocks of the 4th round input. Since all the even-numbered inputs of the 4th round have a non-zero difference, all the odd-numbered outputs of the 4th round without round permutation also have a non-zero difference. Therefore, all the outputs of the 4th round have a non-zero difference. □

Figure 8.2 shows an example of a propagation of the input $x_3^{(r)}$ to the output $y_i^{(r+3)}$ for GFN_6 using π^{SD}. In the figure, the dotted lines show partial affection of the input $x_3^{(r)}$ and the bold lines show full affection of the input $x_3^{(r)}$. It is clear from the figure that all of the 4th-round output $y_i^{(r+3)}$ are affected by the input $x_3^{(r)}$. Similarly to this, all of the

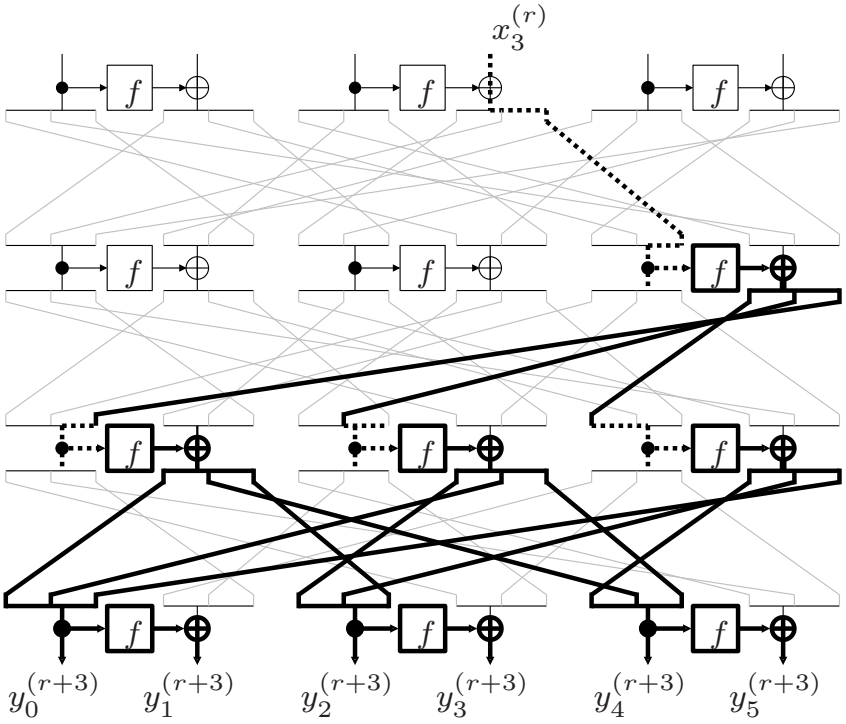

Figure 8.2: GFN_6 using π^{SD}

4th-round output are affected by all of the 1st-round input. Theorem 15 holds as long as each even sub-block is divided into $(d/2)$ blocks and permuted to each odd sub-block input in the next round, and vice versa. We remark that π^{SD} is not the only example of a permutation that has this property. However, since π^{SD} does not destroy the involution property in which the encryption process is almost identical to the decryption process, we consider only π^{SD} in this chapter.

8.3.2 Discussion

While the number of partition for each sub-block of π^{SD} is $(d/2)$ which is optimal regarding DRmax, the round diffusion is improved compared to sub-block wise round permutation when dividing and distributing each sub-block into more than two smaller blocks.

Since the round permutation with sub-block dividing is not a sub-block wise permutation, it demolishes the sub-block structure and thus may improve the security against cryptanalysis exploiting strong sub-block based structure such as saturation attacks. Moreover, it does not increase the implementation cost for hardware implementation in general, since it can be implemented by simple wire connection. On the other hand, in general, the security evaluation including counting the number of active F-functions and finding impossible differential paths for GFN with π^{SD} is harder than that of GFN with a sub-block wise round permutation, especially for large d. Also, the software implementation of π^{SD} might be less efficient than that of sub-block wise permutation. We discuss improving the sub-block wise round permutation in the next section.

8.4 Improving the Diffusion Round by Multiple Round Permutation

In this section, we propose to use multiple round permutations instead of a single round permutation to improve the diffusion round of GFN.

8.4.1 Evaluation for DRmax of $\mathbf{GFN}_d^{\mathbf{2RP}}$

The existence of the corresponding DRmax is efficiently checked by using the algorithm proposed in [DFLM19]. For accurate analysis, DRmax of GFN needs to be evaluated in both encryption and decryption directions. Similarly to this, for $\mathrm{GFN}_d^{\mathrm{2RP}}$, the GFN starting from an even-round and odd-round are also required to be evaluated in addition to encryption and decryption directions. Thus, DRmax of $\mathrm{GFN}_d^{\mathrm{2RP}}$ is given as the maximum of these four values of DRmax (i.e., DRmax of encryption starting from even and odd round, and decryption starting from even and odd round). For a given combination of permutations π_0 and π_1, if the maximum of those four DRmax reaches the theoretical bound given in Proposition 11, the combination of the permutations is considered as tight.

8.4.2 Results on 10-Line GFN with Double Round Permutation ($\mathbf{GFN}_{10}^{\mathbf{2RP}}$)

We exhaustively search all possible two different round permutations for $\mathrm{GFN}_{10}^{\mathrm{2RP}}$. The number of such permutations is $(5!)^4 \approx 2^{26.9}$. As a result, a tight combination of permutations is not found in any two different round permutations. However, combinations partially reaching the lower bound of DRmax (= 6) are found. One of those optimal $\mathrm{GFN}_{10}^{\mathrm{2RP}}$ (denoted as $\mathrm{GFN}_{10}^{\mathrm{2RP}}$-I) is given as follows:

$$\pi_0 = \{1,4,5,8,7,0,9,2,3,6\}, p_0 = \{0,2,3,4,1\}, q_0 = \{2,4,0,1,3\},$$
$$\pi_1 = \{1,8,3,4,7,0,9,2,5,6\}, p_1 = \{0,1,3,4,2\}, q_1 = \{4,2,0,1,3\}.$$

For the optimal $\mathrm{GFN}_{10}^{\mathrm{2RP}}$-I starting from even r (i.e. the first round permutation is π_0), DRmax of the encryption function is 6 which is the lower bound on DRmax for GFN_{10}. The DRmax of the inverse of $\mathrm{GFN}_{10}^{\mathrm{2RP}}$-I starting from even r (i.e. the first round permutation is π_0^{-1}) also achieves DRmax = 6. However, DRmax of $\mathrm{GFN}_{10}^{\mathrm{2RP}}$-I starting from odd r is both 7 for encryption and decryption. Therefore, $\mathrm{GFN}_{10}^{\mathrm{2RP}}$-I is not considered as a fully tight combination of permutations, but partially tight.

Since DRmax of the previously known optimal results for $\mathrm{GFN}_{10}^{\mathrm{1RP}}$ is 7, $\mathrm{GFN}_{10}^{\mathrm{2RP}}$-I partially improves the diffusion compared to $\mathrm{GFN}_{10}^{\mathrm{1RP}}$. The improvement of the security of $\mathrm{GFN}_{10}^{\mathrm{2RP}}$-I depends on the number of rounds when considering actual attacks. However, regarding DRmax, $\mathrm{GFN}_{10}^{\mathrm{2RP}}$-I is better than the previously known optimal $\mathrm{GFN}_{10}^{\mathrm{1RP}}$.

8.4.3 Results on 12-Line GFN with Double Round Permutation ($\mathbf{GFN}_{12}^{\mathbf{2RP}}$)

Similarly to $\mathrm{GFN}_{10}^{\mathrm{2RP}}$, we exhaustively search two different round permutations for $\mathrm{GFN}_{12}^{\mathrm{2RP}}$. We show that there does exist a tight combination of round permutations that reaches

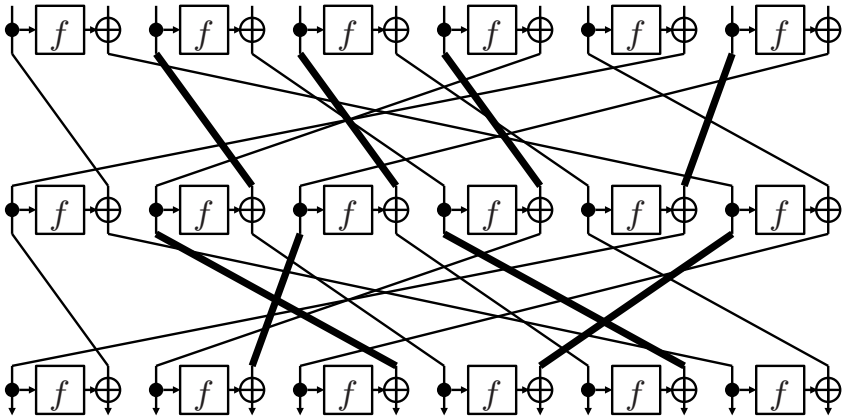

Figure 8.3: Optimal $\mathrm{GFN}_{12}^{2\mathrm{RP}}$ achieving the lower bounds

the lower bound on DRmax for $d = 12$, which is DRmax $= 7$. One of those tight $\mathrm{GFN}_{12}^{2\mathrm{RP}}$ (denoted as $\mathrm{GFN}_{12}^{2\mathrm{RP}}$-I) is given as follows (see also Fig. 8.3):

$$\pi_0 = \{1, 10, 3, 6, 5, 8, 7, 2, 11, 0, 9, 4\}, p_0 = \{0, 1, 2, 3, 5, 4\}, q_0 = \{5, 3, 4, 1, 0, 2\},$$

$$\pi_1 = \{1, 10, 5, 6, 3, 8, 9, 2, 11, 0, 7, 4\}, p_1 = \{0, 2, 1, 4, 5, 3\}, q_1 = \{5, 3, 4, 1, 0, 2\}.$$

DRmax of $\mathrm{GFN}_{12}^{2\mathrm{RP}}$-I starting from any round is 7, which is the lower bound on DRmax for GFN_{12}. We found 28,800 of such tight permutations in all possible two different round permutations.

While $\mathrm{GFN}_{12}^{2\mathrm{RP}}$ requires two different round permutations, for the optimal $\mathrm{GFN}_{12}^{2\mathrm{RP}}$-I, the difference of the two permutations is only four sub-block permutations (i.e. eight sub-block permutations are unchanged). Those differences are illustrated in bold lines in Fig. 8.3. This reduces the implementation overhead for multiple round permutations. Moreover, 48-bit and 96-bit block ciphers, which are known as suitable for RFID (e.g. PRINTcipher [KLPR10]), are directly derived from $\mathrm{GFN}_{12}^{2\mathrm{RP}}$ with 4-bit and 8-bit F-functions (S-boxes). Those imply the practical usefulness of $\mathrm{GFN}_{12}^{2\mathrm{RP}}$.

8.4.4 Discussion

Our result on $\mathrm{GFN}_{12}^{2\mathrm{RP}}$ presents the first GFN that achieves the theoretical lower bound on DRmax. Since $\mathrm{GFN}^{2\mathrm{RP}}$ uses sub-block wise permutations unlike π^{SD}, we can use the existing techniques to evaluate its security including counting the numbers of active F-functions, impossible differential search by $\mathcal{U}$-method [KHS+03, KHL10], and saturation search [BS01, SSA+07]. The implementation of $\mathrm{GFN}^{2\mathrm{RP}}$ is slightly less efficient than that of $\mathrm{GFN}^{1\mathrm{RP}}$ when using round-based implementation for both software and hardware due to non-identical round permutations. However, the implementation cost of the round permutation is not usually dominant in a whole symmetric key primitive implementation. Moreover, when using unrolled implementation in both software and hardware, the efficiency of $\mathrm{GFN}^{2\mathrm{RP}}$ is almost the same as that of $\mathrm{GFN}^{1\mathrm{RP}}$.

Since the search space of the round permutations is rapidly increased for $\mathrm{GFN}^{2\mathrm{RP}}$, it is hard to find optimal two different round permutations for large d of GFN_d by exhaustive

search. However, our result on $\mathrm{GFN}^{2\mathrm{RP}}$ shows a possibility of further improving the diffusion of GFN even if there do not exist tight round permutations in $\mathrm{GFN}^{1\mathrm{RP}}$. Also, its implementation cost is not much increased compared to $\mathrm{GFN}^{1\mathrm{RP}}$. Thus, we believe that our result is useful not only in theory but also in practice.

8.5 Conclusions

We proposed two approaches to improve the round diffusion of d-line GFN. The first approach uses the technique called sub-block dividing which divides each sub-block of GFN_d into $(d/2)$ smaller blocks and appropriately distributes them by the round permutation. We proved that the diffusion round of GFN_d using round permutations with sub-block dividing is always four. The second approach alternately uses two different round permutations instead of a single round permutation. We found the first even-odd permutations that achieve the lower bound on DRmax for 12-line GFN.

Our first result holds regardless of the number of sub-blocks, and it can be incorporated into actual designs of a primitive. Our second result demonstrates the possibility of improving the round diffusion of GFN by using multiple permutations, and tight permutations are obtained for $d = 12$. For $d = 10$, our result shows that only partial tightness can be achieved, and we leave it open the (non-)existence of tight permutations if we use more than three permutations.

Chapter 9

Conclusions and Open Problems

9.1 Conclusions

In this thesis, we have explored the cryptographic properties of Feistel-type symmetric-key cryptosystem from a design and cryptanalysis point of view to design a secure and efficient block cipher. We focused on the diffusion properties of several Feistel structures including balanced Feistel networks (BFNs) and generalized Feistel networks (GFNs). While those structures have several desirable implementation properties, one of the disadvantages compared to substitution permutation networks (SPNs) is its slow diffusion. Therefore, improving the diffusion of Feistel structures allows us to design a more secure and efficient block cipher.

In order to improve the diffusion of Feistel structures, we considered mainly three approaches. The first approach is improving the evaluation methods on the security of Feistel structures related to the diffusion property. Our methods enable us to more accurately evaluate the minimum numbers of active S-boxes for Feistel structures. While this approach does not require to modify the components, the number of required iterations can be reduced by derived accurate results. Thus, as a result, this approach also contributes to improve the diffusion of Feistel structure. The second approach is directly improving the diffusion property by appropriately modifying the underlying F-functions. In this approach, we have showed more efficient F-functions regarding the diffusion for 3-line GFNs, 4-line type-I GFNs and 4-line type-II GFNs compared to the previously known F-function designs for them. Moreover, we have found the theoretically optimal constructions regarding the minimum number of active S-boxes for F-functions of BFNs among SP-type F-functions. Similarly to the second approach, the third approach is improving the diffusion by appropriately modifying the underlying round permutations. It was showed that the diffusion property can be improved by alternately using different round permutations in each round. Moreover, we have showed the first result achieving the lower bound on the maximum diffusion round by using our proposed permutations.

In summary, from Chapters 4 to 8, we have dealt with the security properties of diffusion used in Feistel-type block ciphers as follows:

- Security evaluations regarding the lower bounds on the number of active S-boxes for BFNs and GFNs are significantly improved by our new evaluation algorithm. Consequently, it allows us to reduce the required number of rounds to provide sufficient diffusion by accurate lower bounds derived from our algorithm (**Chapter 4**).

- For 3-line GFNs, it was shown that the underlying F-function consisting of double SP-functions has better diffusion with respect to the proportion of active S-boxes compared to the F-function consisting of single SP-functions. This implies that there exists a better design regarding the diffusion for F-function of 3-line GFNs which is superior to the previously known F-function designs. This opens up the possibility of designing more efficient ciphers based on 3-line GFNs (**Chapter 5**).

- For 4-line GFNs, it was shown that type-I and type-II constructions are the best regarding the diffusion among all possible connections of 4-line GFNs. Moreover, our newly proposed constructions which are 4-line type-I and type-II GFNs with the underlying F-functions consisting of SPS-functions or double SP-functions have better proportion of active S-boxes compared to those consisting of single SP-functions. This result shows that there exists a better design for F-functions of 4-line type-I and type-II GFNs compared to the previously known designs (**Chapter 6**).

- For BFNs, it was proved that the underlying F-function consisting of SPS- or SPSP-functions has optimal diffusion among the F-function consisting of $(\mathrm{SP})^u$ and $(\mathrm{SP})^u\mathrm{S}$ with respect to the proportion of active S-boxes, where u is an arbitrary positive integer. This result showed the optimal design regarding the proportion of active S-boxes of F-functions for BFNs among all possible SP-type F-functions assuming that the underlying diffusion matrix is MDS (**Chapter 7**).

- For some type-II GFNs, it was shown that the diffusion property with respect to the maximum diffusion round of them is improved by alternately using two different round permutations which was not addressed before. As a result, it was shown that there exists a possibility to further improve the diffusion by using two or more round permutations instead of single round permutations. Moreover, our result on a 12-line GFNs is the first result that achieves the lower bound on the maximum diffusion round for GFNs (**Chapter 8**).

One of the direct applications of these results is designing a secure and efficient Feistel-type symmetric-key primitives. Moreover, the results are useful for a deeper understanding the security and theoretical limitations of Feistel-type cryptosystems.

The results in this thesis have been presented in [Shi10, BS11b, BS11a, BS13, SB14, SI22], and they correspond to Chapters 4, 5, 6, 6, 7 and 8, respectively.

9.2 Open Problems

There still exist many open problems on design and analysis of Feistel-type symmetric-key cryptosystems. We list some of them as follows for the future work:

- We investigated two metrics on the diffusion property for Feistel-type structures. One is the minimum numbers of active S-boxes which was presented in Chapters 4 to 7. The other is the maximum diffusion round DRmax which was presented in Chapter 8. Both metrics are used for evaluations of the diffusion property. However, the theoretical relation between the minimum numbers of active S-boxes and DRmax still remains an open problem.

- In Chapter 8, we found several round permutations that achieve the theoretical lower bounds on DRmax for GFNs with even-odd permutations. However, in general, the existence of round permutations that achieve the theoretical lower bounds for several GFNs has not been known. For example, it is still unclear whether there exists a 10-line GFN with DRmax = 6, while it has been known by exhaustive search that 10-line GFNs with any single round permutation cannot achieve DRmax = 6. Moreover, generic construction for optimal round permutations for GFNs with large blocks (e.g. 32-line) is also unknown.

- Our algorithm described in Fig. 4.12 of Chapter 4 can find much better solutions for the minimum number of active S-boxes for BFNs and GFNs than the previous approaches. However, the derived solutions are not usually the best ones. Thus, the algorithm that finds the best solution for the minimum number of active S-boxes for BFNs and GFNs is still unknown. Moreover, our algorithm may be further improved by applying MILP (Mixed integer linear programming).

- Most of the results on the minimum number of active S-boxes presented in Chapters 4 to 7 were only proven to be tight assuming that the underlying diffusion matrix is MDS. The tight bounds on the number of active S-boxes when the underlying diffusion matrix for BFNs and GFNs is non-MDS have not been presented.

List of Abbreviations and Notations

Abbreviations

- ARX: Addition-Rotation-XOR
- GFN: Generalized Feistel network
- BFN: Balanced Feistel network
- MDS: Maximum distance separable
- PRF: Pseudo random function
- PRP: Pseudo random permutation
- SPN: Substitution Permutation Network
- SP: Substitution-Permutation
- SPS: Substitution-Permutation-Substitution (two substitution layers separated by a permutation layer)
- TLS: Transport layer security

Notations

- $x_j^{(i)}, y_j^{(i)}$: input and output of the j-th S-box layer in the i-th round.
- $z_j^{(i)}$: output of the j-th linear diffusion layer in the i-th round.
- $\Delta x_j^{(i)}$: a difference of $x_j^{(i)}$.
- $dw_j^{(i)}$: a truncated difference weight of $x_j^{(i)}$, i.e., $dw_j^{(i)} = w_n(\Delta x_j^{(i)})$.
- $dw^{(i)}$: the number of differentially active S-boxes in the i-th round.
- $\mathcal{D}(r)$: the minimum number of active S-boxes in r consecutive rounds.
- $\Gamma y_j^{(i)}$: a linear mask value of $y_j^{(i)}$.
- $\delta x_j^{(i)}$: a truncated differential of $x_j^{(i)}$.

- $\gamma y_j^{(i)}$: a truncated linear mask value of $y_j^{(i)}$.
- GFN_d: a d-block (or d-line) generalized Feistel network (see Section 3.1.3 for details).
- $\mathcal{NS}_{m,r}$: number of all S-boxes in r rounds when each S-layer consists of m S-boxes in parallel.
- $\mathcal{NA}_{m,r}$: minimum number of active S-boxes in r rounds when each S-layer consists of m S-boxes in parallel.
- $\mathcal{E}_m$: $\lim_{r\to\infty} \frac{\mathcal{NA}_{m,r}}{\mathcal{NS}_{m,r}}$.
- $\mathcal{E}$: $\lim_{r\to\infty} \mathcal{E}_m$.
- π: a round permutation $\pi : \{\{0,1\}^{mn}\}^d \to \{\{0,1\}^{mn}\}^d$.
- π_e: an even-odd permutation.
- π_o: an odd-even permutation.

Bibliography

[Ada97a] Carlisle Adams. The CAST-128 encryption algorithm. *RFC*, 2144:1–15, 1997.

[Ada97b] Carlisle M. Adams. Constructing symmetric ciphers using the CAST design procedure. *Des. Codes Cryptogr.*, 12(3):283–316, 1997.

[AG99] Carlisle Adams and Jeff Gilchrist. The CAST-256 encryption algorithm. *RFC*, 2612:1–19, 1999.

[AIK+00] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis. In Douglas R. Stinson and Stafford E. Tavares, editors, *Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 14-15, 2000, Proceedings*, volume 2012 of *Lecture Notes in Computer Science*, pages 39–56. Springer, 2000.

[AO97] Kazumaro Aoki and Kazuo Ohta. Strict evaluation of the maximum average of differential probability and the maximum average of linear probability. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 80-A(1):2–8, 1997.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 411–436. Springer, 2015.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 12–23. Springer, 1999.

[BCD+99] Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M. Matyas Jr., Luke O'Connor, Mohammad Peyravian, David Safford, and Nevenko Zunic. MARS - a candidate cipher for AES. IBM Corporation, 1999.

[BDK01] Eli Biham, Orr Dunkelman, and Nathan Keller. The rectangle attack - rectangling the Serpent. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*, pages 340–357. Springer, 2001.

[BDLF10] Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent, and Pierre-Alain Fouque. Attacks on hash functions based on generalized Feistel: Application to reduced-round Lesamnta and SHAvite-3_{512}. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers*, volume 6544 of *Lecture Notes in Computer Science*, pages 18–35. Springer, 2010.

[Bih94] Eli Biham. On Matsui's linear cryptanalysis. In Alfredo De Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 341–355. Springer, 1994.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[BKR97] Johan Borst, Lars R. Knudsen, and Vincent Rijmen. Two attacks on reduced IDEA. In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 1997.

[Bog10] Andrey Bogdanov. On the differential and linear efficiency of balanced Feistel networks. *Inf. Process. Lett.*, 110(20):861–866, 2010.

[Bog11] Andrey Bogdanov. On unbalanced Feistel networks with contracting MDS diffusion. *Des. Codes Cryptogr.*, 59(1-3):35–58, 2011.

[BR10] Andrey Bogdanov and Christian Rechberger. A 3-subset meet-in-the-middle attack: Cryptanalysis of the lightweight block cipher KTANTAN. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers*, volume 6544 of *Lecture Notes in Computer Science*, pages 229–240. Springer, 2010.

[BR11] Paulo S. L. M. Barreto and Vincent Rijmen. Whirlpool. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security, 2nd Ed*, pages 1384–1385. Springer, 2011.

[BR14] Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Des. Codes Cryptogr.*, 70(3):369–383, 2014.

[BRS02] John Black, Phillip Rogaway, and Thomas Shrimpton. Black-box analysis of the block-cipher-based hash-function constructions from PGV. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 320–335. Springer, 2002.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptol.*, 4(1):3–72, 1991.

[BS93] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993.

[BS01] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*, pages 394–405. Springer, 2001.

[BS11a] Andrey Bogdanov and Kyoji Shibutani. Analysis of 3-line generalized Feistel networks with double SD-functions. *Inf. Process. Lett.*, 111(13):656–660, 2011.

[BS11b] Andrey Bogdanov and Kyoji Shibutani. Double SP-functions: Enhanced generalized Feistel networks - extended abstract. In Udaya Parampalli and Philip Hawkes, editors, *Information Security and Privacy - 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings*, volume 6812 of *Lecture Notes in Computer Science*, pages 106–119. Springer, 2011.

[BS13] Andrey Bogdanov and Kyoji Shibutani. Generalized Feistel networks revisited. *Des. Codes Cryptogr.*, 66(1-3):75–97, 2013.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. *IACR Cryptol. ePrint Arch.*, page 404, 2013.

[BW12] Andrey Bogdanov and Meiqin Wang. Zero correlation linear cryptanalysis with reduced data complexity. In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 29–48. Springer, 2012.

[CGT19] Victor Cauchois, Clément Gomez, and Gaël Thomas. General diffusion analysis: How to find optimal permutations for generalized type-ii Feistel schemes. *IACR Trans. Symmetric Cryptol.*, 2019(1):264–301, 2019.

[Cop94] Don Coppersmith. The data encryption standard (DES) and its strength against attacks. *IBM J. Res. Dev.*, 38(3):243–250, 1994.

[CY09] Jiali Choy and Huihui Yap. Impossible boomerang attack for block cipher structures. In Tsuyoshi Takagi and Masahiro Mambo, editors, *Advances in Information and Computer Security, 4th International Workshop on Security, IWSEC 2009, Toyama, Japan, October 28-30, 2009, Proceedings*, volume 5824 of *Lecture Notes in Computer Science*, pages 22–37. Springer, 2009.

[DB09] Orr Dunkelman and Eli Biham. The SHAvite-3 - A new hash function. In Helena Handschuh, Stefan Lucks, Bart Preneel, and Phillip Rogaway, editors, *Symmetric Cryptography, 11.01. - 16.01.2009*, volume 09031 of *Dagstuhl Seminar Proceedings*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany, 2009.

[DFLM19] Patrick Derbez, Pierre-Alain Fouque, Baptiste Lambin, and Victor Mollimard. Efficient search for optimal diffusion layers of generalized Feistel networks. *IACR Trans. Symmetric Cryptol.*, 2019(2):218–240, 2019.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher SQUARE. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.

[DR01] Joan Daemen and Vincent Rijmen. The wide trail design strategy. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, volume 2260 of *Lecture Notes in Computer Science*, pages 222–238. Springer, 2001.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[Fei73] Horst Feistel. Cryptography and Computer Privacy. *Scientific American*, 228:1523, 1973.

[HCS+06] Deukjo Hong, Donghoon Chang, Jaechul Sung, Sangjin Lee, Seokhie Hong, Jaesang Lee, Dukjae Moon, and Sungtaek Chee. A new dedicated 256-bit hash function: FORK-256. In Matthew J. B. Robshaw, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*, pages 195–209. Springer, 2006.

[HKY00] Shoichi Hirose, Hidenori Kuwakado, and Hirotaka Yoshida. SHA-3 proposal: Lesamnta, 2000.

[HLL+00] Seokhie Hong, Sangjin Lee, Jongin Lim, Jaechul Sung, Dong Hyeon Cheon, and Inho Cho. Provable security against differential and linear cryptanalysis for the SPN structure. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 273–283. Springer, 2000.

[HSH+06] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee. HIGHT: A new block cipher suitable for low-resource device. In Louis Goubin and Mitsuru Matsui, editors, *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, volume 4249 of *Lecture Notes in Computer Science*, pages 46–59. Springer, 2006.

[JK97] Thomas Jakobsen and Lars R. Knudsen. The interpolation attack on block ciphers. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 28–40. Springer, 1997.

[Kan00] Masayuki Kanda. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function. In Douglas R. Stinson and Stafford E. Tavares, editors, *Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 14-15, 2000, Proceedings*, volume 2012 of *Lecture Notes in Computer Science*, pages 324–338. Springer, 2000.

[Ker83] Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:161–191, 1883.

[KHL+01] Ju-Sung Kang, Seok-Hie Hong, Sang-Jin Lee, Ok-Yeon Yi, Choon-Sik Park, and Jong-In Lim. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks. In *ETRI Journal*, volume 23, pages 158–167, 2001.

[KHL10] Jongsung Kim, Seokhie Hong, and Jongin Lim. Impossible differential cryptanalysis using matrix method. *Discret. Math.*, 310(5):988–1002, 2010.

[KHS+03] Jongsung Kim, Seokhie Hong, Jaechul Sung, Changhoon Lee, and Sangjin Lee. Impossible differential cryptanalysis for block cipher structures. In Thomas Johansson and Subhamoy Maitra, editors, *Progress in Cryptology - INDOCRYPT 2003, 4th International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003, Proceedings*, volume 2904 of *Lecture Notes in Computer Science*, pages 82–96. Springer, 2003.

[KKS00] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York,*

NY, USA, April 10-12, 2000, Proceedings, volume 1978 of *Lecture Notes in Computer Science*, pages 75–93. Springer, 2000.

[KLPR10] Lars R. Knudsen, Gregor Leander, Axel Poschmann, and Matthew J. B. Robshaw. PRINTcipher: A block cipher for IC-printing. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*, volume 6225 of *Lecture Notes in Computer Science*, pages 16–32. Springer, 2010.

[KLS+08] Jongsung Kim, Changhoon Lee, Jaechul Sung, Seokhie Hong, Sangjin Lee, and Jongin Lim. Seven new block cipher structures with provable security against differential cryptanalysis. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 91-A(10):3047–3058, 2008.

[KMA+00] Masayuki Kanda, Shiho Moriai, Kazumaro Aoki, Hiroki Ueda, Youichi Takashima, Kazuo Ohta, and Tsutomu Matsumoto. E2 a new 128-bit block cipher. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 83-A(1):48–59, 2000.

[Knu94] Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer, 1994.

[LDKK08] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New impossible differential attacks on AES. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *Progress in Cryptology - INDOCRYPT 2008, 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. Proceedings*, volume 5365 of *Lecture Notes in Computer Science*, pages 279–293. Springer, 2008.

[LH94] Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. In Yvo Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 17–25. Springer, 1994.

[LKS+06] Changhoon Lee, Jongsung Kim, Jaechul Sung, Seokhie Hong, and Sangjin Lee. Provable security for an RC6-like structure and a MISTY-FO-like structure against differential cryptanalysis. In Marina L. Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Kenneth Tan, David Taniar, Antonio Laganà, Youngsong Mun, and Hyunseung Choo, editors, *Computational Science and Its Applications - ICCSA 2006, International Conference, Glasgow, UK, May 8-11, 2006, Proceedings, Part III*, volume 3982 of *Lecture Notes in Computer Science*, pages 446–455. Springer, 2006.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of mathematics and its applications*. Cambridge University Press, 1997.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[Luc01] Stefan Lucks. The saturation attack - A bait for Twofish. In Mitsuru Matsui, editor, *Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers*, volume 2355 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2001.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

[Mat94] Mitsuru Matsui. On correlation between the order of S-boxes and the strength of DES. In Alfredo De Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 366–375. Springer, 1994.

[Mat96] Mitsuru Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. In Dieter Gollmann, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings*, volume 1039 of *Lecture Notes in Computer Science*, pages 205–218. Springer, 1996.

[Mat97] Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 54–68. Springer, 1997.

[Mau92] Ueli M. Maurer. A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generator. In Rainer A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings*, volume 658 of *Lecture Notes in Computer Science*, pages 239–255. Springer, 1992.

[Miy90] Shoji Miyaguchi. The FEAL cipher family. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 627–638. Springer, 1990.

[MSS11] Kazuhiko Minematsu, Tomoyasu Suzaki, and Maki Shigeri. On maximum differential probability of generalized Feistel. In Udaya Parampalli and Philip Hawkes, editors, *Information Security and Privacy - 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings*,

volume 6812 of *Lecture Notes in Computer Science*, pages 89–105. Springer, 2011.

[MV00] Shiho Moriai and Serge Vaudenay. On the pseudorandomness of top-level schemes of block ciphers. In Tatsuaki Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings*, volume 1976 of *Lecture Notes in Computer Science*, pages 289–302. Springer, 2000.

[Nat77] National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards (FIPS) Publication 46, 1977.

[Nat94] National Soviet Bureau of Standards. Information processing system - cryptographic protection - cryptographic algorithm GOST 28147-89, 1994.

[Nat01a] National Institute of Standards and Tehcnology (NIST). Advanced Encryption Standard. Federal Information Processing Standards (FIPS) Publication 197, 2001.

[Nat01b] National Institute of Standards and Tehcnology (NIST). Recommendation for Block Cipher Modes of Operation: Methods and Techniques. Special Publication 800-38A, 2001.

[Nat02] National Institute of Standards and Technology (NIST). Secure Hash Standard. Federal Information Processing Standards (FIPS) Publication 180-2, 2002.

[Nat07a] National Institute of Standards and Tehcnology (NIST). Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Special Publication 800-38D, 2007.

[Nat07b] National Institute of Standards and Tehcnology (NIST). Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality. Special Publication 800-38C, 2007.

[Nat10] National Institute of Standards and Tehcnology (NIST). Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices. Special Publication 800-38E, 2010.

[Nat16] National Institute of Standards and Tehcnology (NIST). Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication. Special Publication 800-38B, 2016.

[NK92] Kaisa Nyberg and Lars R. Knudsen. Provable security against differential cryptanalysis. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 566–574. Springer, 1992.

[NK95] Kaisa Nyberg and Lars R. Knudsen. Provable security against a differential attack. *J. Cryptol.*, 8(1):27–37, 1995.

[NW97] Roger M. Needham and David J. Wheeler. Tea extensions. Techniacl report, Computer Laboratory, University of Cambridge, October 1997. Available at http://www.cix.co.uk/~klockstone/xtea.pdf.

[Nyb93] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer, 1993.

[Nyb96] Kaisa Nyberg. Generalized Feistel networks. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, volume 1163 of *Lecture Notes in Computer Science*, pages 91–104. Springer, 1996.

[PGV93] Bart Preneel, René Govaerts, and Joos Vandewalle. Hash functions based on block ciphers: A synthetic approach. In Douglas R. Stinson, editor, *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, volume 773 of *Lecture Notes in Computer Science*, pages 368–378. Springer, 1993.

[Pha04] Raphael Chung-Wei Phan. Impossible differential cryptanalysis of 7-round advanced encryption standard (AES). *Inf. Process. Lett.*, 91(1):33–38, 2004.

[Pie90] Josef Pieprzyk. How to construct pseudorandom permutations from single pseudorandom functions. In Ivan Damgård, editor, *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of of Cryptographic Techniques, Aarhus, Denmark, May 21-24, 1990, Proceedings*, volume 473 of *Lecture Notes in Computer Science*, pages 140–150. Springer, 1990.

[PSC+02] Sangwoo Park, Soo Hak Sung, Seongtaek Chee, E-Joong Yoon, and Jongin Lim. On the security of Rijndael-like structures against differential and linear cryptanalysis. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 176–191. Springer, 2002.

[PSLL03] Sangwoo Park, Soo Hak Sung, Sangjin Lee, and Jongin Lim. Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES. In Thomas Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*, pages 247–260. Springer, 2003.

[RDP+96] Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers, and Erik De Win. The cipher SHARK. In Dieter Gollmann, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings*, volume 1039 of *Lecture Notes in Computer Science*, pages 99–111. Springer, 1996.

[Res18] Eric Rescorla. The transport layer security (TLS) protocol version 1.3. *RFC*, 8446:1–160, 2018.

[Riv98] Ron Rivest. A description of the RC2(r) encryption algorithm. *RFC*, 2268:1–11, 1998.

[RRY00] Ronald L. Rivest, Matthew J. B. Robshaw, and Yiqun Lisa Yin. RC6 as the AES. In *The Third Advanced Encryption Standard Candidate Conference, April 13-14, 2000, New York, New York, USA*, pages 337–342. National Institute of Standards and Technology,, 2000.

[SA08] Taizo Shirai and Kiyomichi Araki. On generalized Feistel structures using the diffusion switching mechanism. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 91-A(8):2120–2129, 2008.

[SB14] Kyoji Shibutani and Andrey Bogdanov. Towards the optimality of Feistel ciphers with substitution-permutation functions. *Des. Codes Cryptogr.*, 73(2):667–682, 2014.

[Sch93] Bruce Schneier. Description of a new variable-length key, 64-bit block cipher (Blowfish). In Ross J. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop, Cambridge, UK, December 9-11, 1993, Proceedings*, volume 809 of *Lecture Notes in Computer Science*, pages 191–204. Springer, 1993.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28(4):656–715, 1949.

[Sha85] Adi Shamir. On the security of DES. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 280–281. Springer, 1985.

[Shi01] Hideo Shimizu. On the security of Feistel cipher with SP-type F function. In *Symposium on Cryptography and Information Security (SCIS) 2001 (in Japanese)*, 2001.

[Shi10] Kyoji Shibutani. On the diffusion of generalized Feistel structures regarding differential and linear cryptanalysis. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers*, volume 6544 of *Lecture Notes in Computer Science*, pages 211–228. Springer, 2010.

[SI22] Kyoji Shibutani and Tetsu Iwata. On the (im)possibility of improving the round diffusion of generalized Feistel structures. *Inf. Process. Lett.*, 174:106197, 2022.

[SIH+11] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An ultra-lightweight blockcipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer Science*, pages 342–357. Springer, 2011.

[SKW+99] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. The Twofish encryption algorithm: A 128-bit block cipher. Wiley Computer Publishing, 1999.

[SM87] Akihiro Shimizu and Shoji Miyaguchi. Fast data encipherment algorithm FEAL. In David Chaum and Wyn L. Price, editors, *Advances in Cryptology - EUROCRYPT '87, Workshop on the Theory and Application of of Cryptographic Techniques, Amsterdam, The Netherlands, April 13-15, 1987, Proceedings*, volume 304 of *Lecture Notes in Computer Science*, pages 267–278. Springer, 1987.

[SM10] Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the generalized Feistel. In Seokhie Hong and Tetsu Iwata, editors, *Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers*, volume 6147 of *Lecture Notes in Computer Science*, pages 19–39. Springer, 2010.

[SMK97] Takeshi Shimoyama, Shiho Moriai, and Toshinobu Kaneko. Improving the higher order differential attack and cryptanalysis of the KN cipher. In Eiji Okamoto, George I. Davida, and Masahiro Mambo, editors, *Information Security, First International Workshop, ISW '97, Tatsunokuchi, Japan, September 17-19, 1997, Proceedings*, volume 1396 of *Lecture Notes in Computer Science*, pages 32–42. Springer, 1997.

[SP04] Taizo Shirai and Bart Preneel. On Feistel ciphers using optimal diffusion mappings across multiple rounds. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2004.

[SS04] Taizo Shirai and Kyoji Shibutani. Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices. In Bimal K. Roy and Willi Meier, editors, *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*, volume 3017 of *Lecture Notes in Computer Science*, pages 260–278. Springer, 2004.

[SS06] Taizo Shirai and Kyoji Shibutani. On Feistel structures using a diffusion switching mechanism. In Matthew J. B. Robshaw, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*, pages 41–56. Springer, 2006.

[SSA+07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In Alex Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.

[TG91] Anne Tardy-Corfdir and Henri Gilbert. A known plaintext attack of FEAL-4 and FEAL-6. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 172–181. Springer, 1991.

[Thi99] Third Generation Partnership Project. Technical specification group services and system aspects, 3G security, specification of the 3GPP confidentiality and integrity algorithms; document 2: KASUMI specification, v3.1.1, 1999.

[TTS+08] Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzaki, and Hiroyasu Kubo. Impossible differential cryptanalysis of CLEFIA. In Kaisa Nyberg, editor, *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 398–411. Springer, 2008.

[Wag99] David A. Wagner. The boomerang attack. In Lars R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.

[WB12] Qingju Wang and Andrey Bogdanov. The provable constructive effect of diffusion switching mechanism in CLEFIA-type block ciphers. *Inf. Process. Lett.*, 112(11):427–432, 2012.

[WZL06] Wenling Wu, Wentao Zhang, and Dongdai Lin. Security on generalized Feistel scheme with SP round function. *Int. J. Netw. Secur.*, 3(3):215–224, 2006.

[ZMI89a] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. Impossibility and optimality results on constructing pseudorandom permutations (extended abstract). In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*, volume 434 of *Lecture Notes in Computer Science*, pages 412–422. Springer, 1989.

[ZMI89b] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 461–480. Springer, 1989.

List of Publications

Main results

1. Kyoji Shibutani. On the diffusion of generalized Feistel structures regarding differential and linear cryptanalysis. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers*, volume 6544 of *Lecture Notes in Computer Science*, pages 211–228. Springer, 2010 (**Chapter 4**).

2. Andrey Bogdanov and Kyoji Shibutani. Analysis of 3-line generalized Feistel networks with double SD-functions. *Inf. Process. Lett.*, 111(13):656–660, 2011 (**Chapter 5**).

3. Andrey Bogdanov and Kyoji Shibutani. Double SP-functions: Enhanced generalized Feistel networks - extended abstract. In Udaya Parampalli and Philip Hawkes, editors, *Information Security and Privacy - 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings*, volume 6812 of *Lecture Notes in Computer Science*, pages 106–119. Springer, 2011 (**Chapter 6**).

4. Andrey Bogdanov and Kyoji Shibutani. Generalized Feistel networks revisited. *Des. Codes Cryptogr.*, 66(1-3):75–97, 2013 (**Chapter 6**).

5. Kyoji Shibutani and Andrey Bogdanov. Towards the optimality of Feistel ciphers with substitution-permutation functions. *Des. Codes Cryptogr.*, 73(2):667–682, 2014 (**Chapter 7**).

6. Kyoji Shibutani and Tetsu Iwata. On the (im)possibility of improving the round diffusion of generalized Feistel structures. *Inf. Process. Lett.*, 174:106197, 2022 (**Chapter 8**).

Other results

1. Taizo Shirai and Kyoji Shibutani. Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices. In Bimal K. Roy and Willi Meier, editors, *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*, volume 3017 of *Lecture Notes in Computer Science*, pages 260–278. Springer, 2004.

2. Taizo Shirai and Kyoji Shibutani. On Feistel structures using a diffusion switching mechanism. In Matthew J. B. Robshaw, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*, pages 41–56. Springer, 2006.

3. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In Alex Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.

4. Toru Akishita, Masanobu Katagi, Yoshikazu Miyato, Asami Mizuno, and Kyoji Shibutani. A practical DPA countermeasure with BDD architecture. In Gilles Grimaud and François-Xavier Standaert, editors, *Smart Card Research and Advanced Applications, 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008. Proceedings*, volume 5189 of *Lecture Notes in Computer Science*, pages 206–217. Springer, 2008.

5. Takanori Isobe and Kyoji Shibutani. Preimage attacks on reduced Tiger and SHA-2. In Orr Dunkelman, editor, *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, volume 5665 of *Lecture Notes in Computer Science*, pages 139–155. Springer, 2009.

6. Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An ultra-lightweight blockcipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer Science*, pages 342–357. Springer, 2011.

7. Takanori Isobe and Kyoji Shibutani. All subkeys recovery attack on block ciphers: Extending meet-in-the-middle approach. In Lars R. Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, volume 7707 of *Lecture Notes in Computer Science*, pages 202–221. Springer, 2012.

8. Ji Li, Takanori Isobe, and Kyoji Shibutani. Converting meet-in-the-middle preimage attack into pseudo collision attack: Application to SHA-2. In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 264–286. Springer, 2012.

9. Takanori Isobe and Kyoji Shibutani. Security analysis of the lightweight block ciphers XTEA, LED and Piccolo. In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, *Information Security and Privacy - 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012. Proceedings*, volume 7372 of *Lecture Notes in Computer Science*, pages 71–86. Springer, 2012.

10. Takanori Isobe and Kyoji Shibutani. Generic key recovery attack on Feistel scheme. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 464–485. Springer, 2013.

11. Takanori Isobe and Kyoji Shibutani. Improved all-subkeys recovery attacks on FOX, KATAN and SHACAL-2 block ciphers. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 104–126. Springer, 2014.

12. Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 411–436. Springer, 2015.

13. Takanori Isobe and Kyoji Shibutani. New key recovery attacks on minimal two-round Even-Mansour ciphers. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 244–263. Springer, 2017.

14. Takanori Isobe and Kyoji Shibutani. Meet-in-the-middle key recovery attacks on a single-key two-round Even-Mansour cipher. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 102-A(1):17–26, 2019.

15. Takanori Isobe and Kyoji Shibutani. Key-recovery security of single-key Even-Mansour ciphers. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 103-A(7):893–905, 2020.