On the Diffusion of Generalized Feistel Structures Regarding Differential and Linear Cryptanalysis

Kyoji Shibutani*

Sony Corporation
1-7-1 Konan, Minato-ku, Tokyo 108-0075, Japan
Kyoji.Shibutani@jp.sony.com

Abstract. This paper studies the security of blockciphers with generalized Feistel structures (GFS) consisting of SP-type F-functions. While GFS leads to compact implementations, the security is not well understood, in particular for larger values of the partitioning number which indicates the number of subblocks. 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 GFS utilizing word-based rotation as a round permutation. These bounds are almost twice as large as the previous results in literature. 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 GFS with large parameters. The proposed algorithm exploits 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. Thus the results enable us to design a more efficient symmetric key primitive. Moreover, we show that the improved GFS proposed by Suzaki and Minematsu at FSE 2010 have more active S-boxes than the standard GFS.

Keywords: blockcipher, generalized Feistel structure, diffusion, lightweight cryptography.

1 Introduction

It is well known that Type-II generalized Feistel structures (GFS) [18] have several desirable implementation properties, notably compactness. For instance, the GFS has smaller F-functions compared to the Feistel structure for the same block size. Also GFS 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 GFS is an attractive structure for a lightweight symmetric key primitive such as a blockcipher or a hash function.

* This work was done while the author stayed at ESAT/COSIC, Katholieke Universiteit Leuven, Belgium.

A. Biryukov, G. Gong, and D.R. Stinson (Eds.): SAC 2010, LNCS 6544, pp. 211–228, 2011.

This might be one of the reasons why recent blockciphers such as CLEFIA [16] and HIGHT [6] utilize the GFS.

The GFS divides a plaintext into d subblocks, where $d > 2$, instead of $d = 2$ as used in Feistel structures. The size of the F-functions used in the GFS depends on the partitioning number d and the block size. If the partitioning number d of the GFS 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.

Recently, Suzaki and Minematsu introduced a GFS with the optimal round permutation with respect to full diffusion property, which is a property that all outputs are affected by all inputs [17]. Their paper showed that the improved GFS can be more secure against impossible differential and saturation attacks than the standard GFS. 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 GFS to be secure against differential and linear attacks [3,10].

It is well understood how to practically evaluate the security against differential and linear attacks by determining the maximum differential and linear characteristic probabilities [4,7]. For instance, counting the number of active S-boxes is a well used technique to evaluate the immunity against those attacks [16]. This approach was used to design many blockciphers and hash functions, including AES [5] and Whirlpool [1]. In SPN structures, it is relatively easy to evaluate the minimum number of active S-boxes by evaluating the permutation layers as discussed in [4]. 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 [7]. Shirai and Araki extended his result to three types of generalized Feistel structures [14], which are known as Type-I, Type-II and Nyberg's constructions [13,18]. They showed that any six consecutive rounds of Type-II GFS with any partitioning number have at least the same number of active S-boxes as the Feistel structure. They also introduced an efficient weight-based active S-box search algorithm. However, their algorithm only works for small parameter sets of the GFS 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 paper, we show the first tight bounds on the minimum number of differential and linear active S-boxes of GFS with large parameter sets. We first prove tight lower bounds for four and six rounds of the standard GFS manually. The obtained bound of six rounds of the standard GFS 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 GFS with large parameters including recently proposed GFS utilizing optimal round permutations [17].

Table 1. Summary of our results, where $\mathcal{B}$ is the differential or the linear branch number of the matrices used in GFS

rounds	Feistel [7,15]	$\mathrm{GFS}_d^{\mathrm{std}}$ [14]	$\mathrm{GFS}_4^{\mathrm{std}}$ **(this paper)**	$\mathrm{GFS}_8^{\mathrm{std}}$ **(this paper)**	$\mathrm{GFS}_6^{\mathrm{imp}}$ **(this paper)**	$\mathrm{GFS}_8^{\mathrm{imp}}$ **(this paper)**
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	$\mathcal{B}+2$	$\mathcal{B}+2$	$\mathbf{2\mathcal{B}+2}$	$\mathbf{2\mathcal{B}+2}$	$\mathbf{2\mathcal{B}+2}$	$\mathbf{2\mathcal{B}+2}$
7	-	-	$\mathbf{2\mathcal{B}+2}$	$\mathbf{2\mathcal{B}+4}$	$\mathbf{2\mathcal{B}+4}$	$\mathbf{2\mathcal{B}+4}$
8	$2\mathcal{B}+1$	-	$\mathbf{2\mathcal{B}+3}$	$\mathbf{3\mathcal{B}+3}$	$\mathbf{4\mathcal{B}+2}$	$\mathbf{4\mathcal{B}+3}$
9	$2\mathcal{B}+2$	-	$\mathbf{2\mathcal{B}+4}$	$\mathbf{3\mathcal{B}+6}$	$\mathbf{4\mathcal{B}+4}$	$\mathbf{4\mathcal{B}+6}$
10	-	-	$\mathbf{3\mathcal{B}+3}$	$\mathbf{4\mathcal{B}+5}$	$\mathbf{4\mathcal{B}+6}$	$\mathbf{5\mathcal{B}+4}$
11	-	-	$\mathbf{3\mathcal{B}+5}$	$\mathbf{4\mathcal{B}+8}$	$\mathbf{4\mathcal{B}+8}$	$\mathbf{5\mathcal{B}+7}$
12	$3\mathcal{B}+1$	$2\mathcal{B}+4$	$\mathbf{4\mathcal{B}+4}$	$\mathbf{6\mathcal{B}+6}$	$\mathbf{6\mathcal{B}+2}$	$\mathbf{7\mathcal{B}+4}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
18	$4\mathcal{B}+4$	$3\mathcal{B}+6$	$\mathbf{6\mathcal{B}+6}$	$\mathbf{8\mathcal{B}+8}$	$\mathbf{8\mathcal{B}+10}$	$\mathbf{10\mathcal{B}+6}$

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 GFS, but also for designing an efficient symmetric primitive. Our results are summarized in Table 1. More detailed results are listed in Appendix A.

This paper is organized as follows. In Sect. 2, definitions and some properties are introduced. In Sect. 3, related work on GFS is explained. Section 4 and 5 describe the lower bounds on the number of differential and linear active S-boxes in GFS, respectively. In Sect. 6, we discuss the result obtained in this paper. Finally, we conclude in Sect. 7.

2 Preliminaries

2.1 Target Structures

In this paper, we focus on GFS with SP-type F-functions [7] and an *even-odd* shuffle [17] as shown in Fig. 1. Let d be an even integer. A dmn-bit plaintext P is divided into d subblocks as $P = (x_0^{(1)}, x_1^{(1)}, ..., x_{d-1}^{(1)})$, where $x_j^{(i)} \in \{0,1\}^{mn}$. Then the i-th round output is calculated as follows:

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

where $F_j^{(i)} : \{0,1\}^{mn} \to \{0,1\}^{mn}$ is a j-th round function in the i-th round, and $\pi : (\{0,1\}^{mn})^d \to (\{0,1\}^{mn})^d$ is a deterministic permutation. We assume that each round function is the SP-type F-function which consists of an mn-bit round

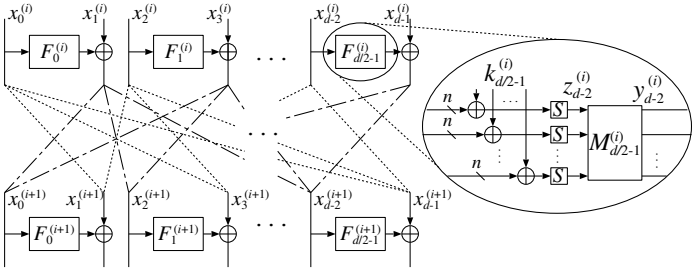

Fig. 1. GFS_d with SP-type F-function and *even-odd* shuffle, where dotted lines show possible connections, each set of outputs and inputs is connected by exactly one line. The sub-diagram on the right is a zoom in on an F-function.

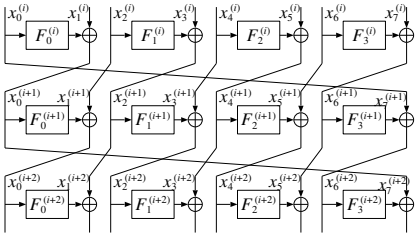

Fig. 2. $\mathrm{GFS}_8^{\mathrm{std}}$

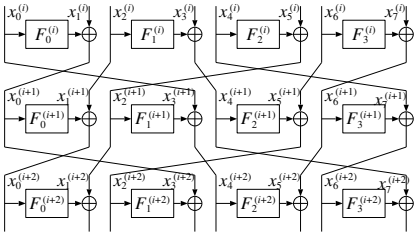

Fig. 3. $\mathrm{GFS}_8^{\mathrm{imp}}$ [17]

key addition, m n-bit bijective S-boxes and an mn-bit linear Boolean function [7]. $S(\cdot)$ 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 GFS with the partitioning number eight and the word-based rotation shown in Fig. 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 paper. Hereafter mn denotes the bit length of subblock, GFS_d denotes the GFS with the partitioning number d, $\mathrm{GFS}_d^{\mathrm{std}}$ denotes the GFS_d with the word-based rotation, i.e., standard Type-II GFS, and $\mathrm{GFS}_d^{\mathrm{imp}}$ denotes the GFS_d with the optimal round permutation proposed by Suzaki and Minematsu [17][1].

2.2 Definitions

In this section, we give some definitions used in the following sections. We first give the definitions of bundle weight and branch number [5].

[1] We treat GFS_d with the round permutations No.1 given in Appendix A of [17] as $\mathrm{GFS}_d^{\mathrm{imp}}$.

Definition 1 (Bundle Weight). *Let* $x \in \{0,1\}^{pn}$ *be represented as* $x=(x_0, x_1, ..., x_{p-1})$*, where* $x_i \in \{0,1\}^n$*, then the bundle weight* $w_n(x)$ *is defined as*

$$w_n(x) = \sharp\{i|0 \leq i \leq p-1, x_i \neq 0\}. \tag{1}$$

Definition 2 (Branch Number). *Let* $P : \{0,1\}^{pn} \rightarrow \{0,1\}^{qn}$*. The branch number of* P *is defined as*

$$\mathcal{B}_n(P) = \min_{a \neq 0}\{w_n(a) + w_n(P(a))\}. \tag{2}$$

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

Definition 3 (Differential Branch Number)

$$\mathcal{B}^D = \min_{1 \leq i \leq r, 0 \leq j \leq d/2-1} \mathcal{B}_n(M_j^{(i)}). \tag{3}$$

Definition 4 (Linear Branch Number)

$$\mathcal{B}^L = \min_{1 \leq i \leq r, 0 \leq j \leq d/2-1} \mathcal{B}_n({}^tM_j^{(i)}), \tag{4}$$

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

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 paper is to clarify the minimum number of differential and linear active S-boxes for GFS 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 [2,11,7]. Thus, in this paper, we mainly discuss the security against differential attacks. We discuss the security against linear attacks in Sect. 5.

2.3 Properties of Generalized Feistel Structures

In this section, we present several properties of GFS. Hereafter 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 GFS have at least one differential active F-function if a non-zero input difference is given.

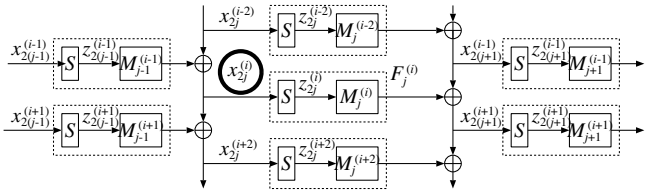

Fig. 4. Five Rounds of $\mathrm{GFS}_d^{\mathrm{std}}$ (Untwisted Form)

We consider the five-round structure of $\mathrm{GFS}_d^{\mathrm{std}}$ shown in Fig. 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

$$D_j^{(i)} = w_n(\Delta x_{2j}^{(i)}) = w_n(\Delta z_{2j}^{(i)}). \tag{5}$$

Then the following property is derived [14].

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

$$M_j^{(i)}(\Delta z_{2j}^{(i)}) = \Delta x_{2(j+1)}^{(i-1)} \oplus \Delta x_{2(j+1)}^{(i+1)}. \tag{6}$$

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

$$w_n(\Delta z_{2j}^{(i)}) \neq 0 \Rightarrow w_n(\Delta z_{2j}^{(i)}) + w_n(\Delta x_{2(j+1)}^{(i-1)}) + w_n(\Delta x_{2(j+1)}^{(i+1)}) \geq \mathcal{B}^D. \tag{7}$$

□

In this paper, 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.

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

$$M_{j-1}^{(i-1)}(\Delta z_{2(j-1)}^{(i-1)}) \oplus \Delta x_{2j}^{(i-2)} = \Delta x_{2j}^{(i)} \neq 0, \tag{8}$$

$$M_{j-1}^{(i-1)}(\Delta z_{2(j-1)}^{(i-1)}) \neq \Delta x_{2j}^{(i-2)}. \tag{9}$$

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 GFS. 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 $\mathrm{GFS}_8^{\mathrm{std}}$ shown in Fig. 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 $\mathrm{GFS}_8^{\mathrm{std}}$ is the identity mapping, and π_O of $\mathrm{GFS}_8^{\mathrm{imp}}$ 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 GFS 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. 2 and 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 GFS_d have at least $w_{mn}(\Delta \boldsymbol{x}^{(i)}) \cdot \mathcal{B}^D$ differential active S-boxes, specifically,

$$\sum_{s=0}^{d/2-1} \sum_{t=i-1}^{i+1} D_s^{(t)} \geq w_{mn}(\Delta \boldsymbol{x}^{(i)}) \cdot \mathcal{B}^D. \tag{10}$$

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 GFS.

3 Related Work

In this section, we discuss previous results related to GFS. The formal definition of GFS was given by Zheng et al. [18]. Several cryptographic properties of these structures were analyzed in [8,12]. Provable security of $\mathrm{GFS}_4^{\mathrm{std}}$ against differential and linear attacks was discussed by Lee et al. [9]. In their results, more than five rounds of $\mathrm{GFS}_4^{\mathrm{std}}$ 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 $\mathrm{GFS}_d^{\mathrm{std}}$ against differential and linear attacks was discussed by Shirai and Araki [14]. They showed the lower bounds on the number of active S-boxes in three types of generalized Feistel structures, Type-I, Type-II and Nyberg's constructions [13,18]. In their results, any six consecutive rounds of $\mathrm{GFS}_d^{\mathrm{std}}$ 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 GFS. Though their algorithm is efficient, still a large computation is required to evaluate large parameter sets of GFS, namely, it requires to search at most $(m+1)^{d(r+1)/2}$ values to evaluate r-round $\mathrm{GFS}_d^{\mathrm{std}}$. Thus the algorithm does not work for $\mathrm{GFS}_d^{\mathrm{std}}$ with large parameters. We use this algorithm to verify the tightness of our results in Sect. 4.4.

Suzaki and Minematsu discussed round permutations of GFS [17]. 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 GFS_d ($d > 4$) could be better than $\mathrm{GFS}_d^{\mathrm{std}}$ by replacing its round permutation from the word-based rotation used in $\mathrm{GFS}_d^{\mathrm{std}}$. In their paper, although the improved GFS has better properties with respect to full diffusion, they have about the same number of active S-boxes[3] as $\mathrm{GFS}_d^{\mathrm{std}}$.

4 Differential Active S-Boxes in GFS

In this section, we present the minimum number of differential active S-boxes in several types of GFS. First, we show better lower bounds for four and six rounds of $\mathrm{GFS}_d^{\mathrm{std}}$. Then, we introduce an exhaustive search algorithm that determines the minimum number of differential active S-boxes for all types of GFS efficiently. By using this algorithm, we present several lower bounds on GFS. 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.

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

Theorem 1. *Let $d \geq 4$. Any four consecutive rounds of $\mathrm{GFS}_d^{\mathrm{std}}$ 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. 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. 5, suppose that

[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.

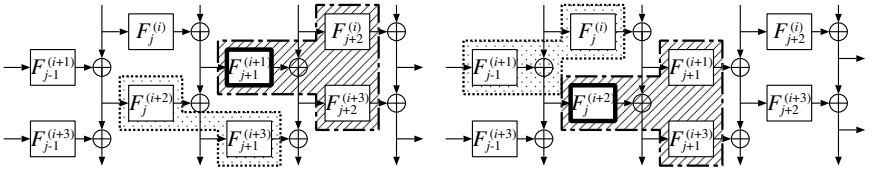

Fig. 5. Four Rounds of $\mathrm{GFS}_d^{\mathrm{std}}$ (Untwisted Form)

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. 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 GFS_d^{std} have at least $2\mathcal{B}^D + 2$ differential active S-boxes.*

See Appendix B for a proof. The bound given by this theorem is almost twice as large as the previous result. Thus, the required number of rounds of $\mathrm{GFS}_d^{\mathrm{std}}$ 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 $\mathrm{GFS}_d^{\mathrm{std}}$ 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 structures can be derived easily. Therefore, we propose another approach to efficiently derive the minimum number of active S-boxes of GFS with large parameter sets in the following section.

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 GFS. This algorithm consists of the following two steps: (a) searching active F-function paths of GFS 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 GFS, then $\mathrm{BD}(R)$ is calculated as follows:

Step 1. Initialize 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 GFS. 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:

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

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. 6. If the bound obtained from the algorithm Fig. 6 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 $\max(\mathrm{Hw}(X^{(2)}) + \mathrm{Hw}(X^{(5)}), \mathrm{Hw}(X^{(3)}), \mathrm{Hw}(X^{(4)}))$, where Hw($X$) denotes a Hamming weight of X. This improvement results in a speed-up in practice.

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 GFS. As discussed in Sect. 2.3, 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 GFS 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 GFS$_d$ 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

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 $S \cdot \mathcal{B}^D + T$

Fig. 6. Algorithm $CountBD(r, X^{(0)}, ..., X^{(r)})$

case, the 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 paper 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. 7 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. 6) outputs $\mathcal{B}^D + 4$ instead of $2\mathcal{B}^D + 2$ as the path in the center of Fig. 7, 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. 7. 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. 7 is not the minimum path for $\mathrm{GFS}_4^{\mathrm{std}}$.

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 [14] 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: $\mathrm{GFS}_4^{\mathrm{std}}$ with $m = 2, 3, ..., 8$,[4]

[4] The case of $\mathrm{GFS}_4^{\mathrm{std}}$ with $m = 4$ is in Table 4 of [14].

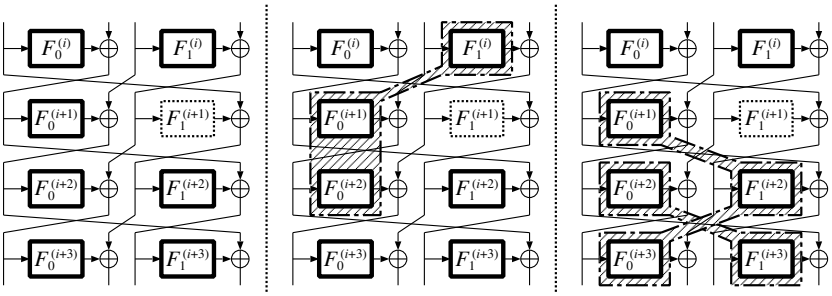

Fig. 7. An Example Path of $\mathrm{GFS}_4^{\mathrm{std}}$

$\mathrm{GFS}_6^{\mathrm{std}}$ with $m = 2, 3, 4$, $\mathrm{GFS}_8^{\mathrm{std}}$ with $m = 2$, $\mathrm{GFS}_6^{\mathrm{imp}}$ with $m = 2, 3, 4$, and $\mathrm{GFS}_8^{\mathrm{imp}}$ 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 computational restrictions of the weight-based exhaustive search, it seems that the obtained bounds are tight as well.

5 Linear Active S-Boxes in GFS

It was shown by Kanda [7] 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 [2,11].

GFS with SP-type F-functions can be represented as GFS with PS-type F-functions in a similar way. Note that, in contrast to Feistel structures, depending on the original round permutation used in GFS, 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 paper: 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 $\mathcal{B}^L$.

6 Discussion

In this section, we discuss the obtained results. We first give an example of the parameter $m = 4$ and $n = 8$ of $\mathrm{GFS}_8^{\mathrm{std}}$, i.e., 256-bit blockcipher, to show

applicability of our results. We assume that this example cipher consists of the MDS matrices and the inversion S-boxes over 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 GFS. 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 $\mathrm{GFS}_4^{\mathrm{std}}$ 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 $\mathrm{GFS}_4^{\mathrm{std}}$ can be represented as active S-boxes in four rounds and six rounds of $\mathrm{GFS}_4^{\mathrm{std}}$. Thus it seems that determining tight bounds for a small 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 GFS 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.

7 Conclusion

In this paper, we have shown the first tight bounds on the minimum number of active S-boxes of GFS with large parameter sets. We first proved tight lower bounds for four and six rounds of the standard GFS manually. Then, we introduced a novel approach to evaluate the minimum number of active S-boxes of GFS 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 GFS can be evaluated precisely, including recently proposed GFS that utilize optimal round permutations instead of the word-based rotation used in the standard GFS. 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 paper depend only on the branch number of the matrices used in GFS. 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 GFS, but also for designing an efficient symmetric key primitive, because the GFS can be implemented compactly and evaluating its security against differential attacks is essential to both blockcipher and hash function design.

Acknowledgments. The author would like to thank Bart Preneel, Nicky Mouha and the anonymous reviewers for their helpful comments.

References

1. Barreto, P.S.L.M., Rijmen, V.: The Whirlpool hashing function. Primitive submitted to NESSIE (September 2000), `http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html` (revised May 2003)
2. Biham, E.: On Matsui's linear cryptanalysis. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 341–355. Springer, Heidelberg (1995)
3. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer, Heidelberg (1993)
4. Daemen, J., Rijmen, V.: The wide trail design strategy. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001)
5. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard (Information Security and Cryptography). Springer, Heidelberg (2002)
6. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S.: HIGHT: A new block cipher suitable for low-resource device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer, Heidelberg (2006)
7. Kanda, M.: Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 324–338. Springer, Heidelberg (2001)
8. Kim, J., Hong, S., Sung, J., Lee, S., Lim, J., Sung, S.: Impossible differential cryptanalysis for block cipher structures. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 82–96. Springer, Heidelberg (2003)
9. Lee, C., Kim, J., Sung, J., Hong, S., Lee, S.: Provable security for an RC6-like structure and a MISTY-FO-like structure against differential cryptanalysis. In: Gavrilova, M., et al. (eds.) ICCSA 2006. LNCS, vol. 3982, pp. 446–455. Springer, Heidelberg (2006)
10. Matsui, M.: Linear cryptanalysis of Data Encryption Standard. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
11. Matsui, M.: On correlation between the order of S-boxes and the strength of DES. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 366–375. Springer, Heidelberg (1995)

12. Moriai, S., Vaudenay, S.: On the pseudorandomness of top-level schemes of block ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 289–302. Springer, Heidelberg (2000)
13. Nyberg, K.: Generalized Feistel network. In: Kim, K., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 91–104. Springer, Heidelberg (1996)
14. Shirai, T., Araki, K.: On generalized Feistel structures using the diffusion switching mechanism. IEICE Trans. Fundamentals E91-A(8), 2120–2129 (2008)
15. Shirai, T., Shibutani, K.: On Feistel structures using a diffusion switching mechanism. In: Robshaw, M.J.B. (ed.) FSE 2006. LNCS, vol. 4047, pp. 41–56. Springer, Heidelberg (2006)
16. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA. In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007)
17. Suzaki, T., Minematsu, K.: Improving the generalized Feistel. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 19–39. Springer, Heidelberg (2010)
18. Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 461–480. Springer, Heidelberg (1990)

A Lower Bounds on the Number of Active S-Boxes

Several lower bounds obtained in this paper are shown in Table 2 and 3. In these tables, $\mathcal{B}$ denotes either the differential or the linear branch number of the matrices used in the GFS.

B A Proof of Theorem 2

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. 8. 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.

Table 2. The Minimum Number of Active S-boxes in $\mathrm{GFS}_d^{\mathrm{std}}$, assuming $\mathcal{B} > 2$

rounds	Feistel	$\mathrm{GFS}_4^{\mathrm{std}}$	$\mathrm{GFS}_6^{\mathrm{std}}$	$\mathrm{GFS}_8^{\mathrm{std}}$	$\mathrm{GFS}_{10}^{\mathrm{std}}$	$\mathrm{GFS}_{12}^{\mathrm{std}}$	$\mathrm{GFS}_{14}^{\mathrm{std}}$	$\mathrm{GFS}_{16}^{\mathrm{std}}$
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 3. The Minimum Number of Active S-boxes in $\mathrm{GFS}_d^{\mathrm{imp}}$, assuming $\mathcal{B} > 2$

rounds	$\mathrm{GFS}_6^{\mathrm{imp}}$	$\mathrm{GFS}_8^{\mathrm{imp}}$	$\mathrm{GFS}_{10}^{\mathrm{imp}}$	$\mathrm{GFS}_{12}^{\mathrm{imp}}$	$\mathrm{GFS}_{14}^{\mathrm{imp}}$	$\mathrm{GFS}_{16}^{\mathrm{imp}}$
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	$8\mathcal{B}+10$	$10\mathcal{B}+6$	$12\mathcal{B}+5$	$12\mathcal{B}+8$	$16\mathcal{B}+3$	$17\mathcal{B}+2$

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.

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 $\mathrm{GFS}_d^{\mathrm{std}}$ 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 $\mathrm{GFS}_d^{\mathrm{std}}$ 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 $\mathrm{GFS}_4^{\mathrm{std}}$ are shown in Figs. 9-13. 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.

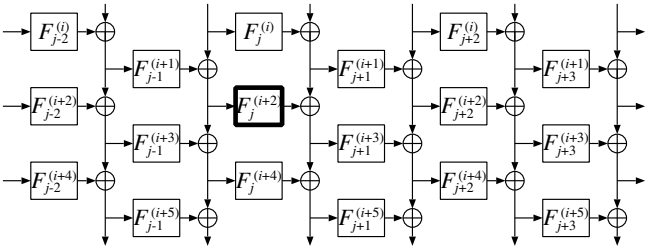

Fig. 8. Six Rounds of $\mathrm{GFS}_d^{\mathrm{std}}$ (Untwisted Form)

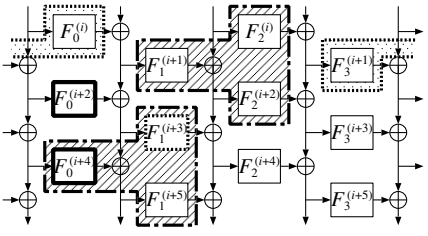

Fig. 9. Case 1-1

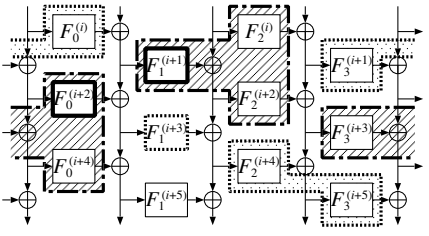

Fig. 10. Case 1-2

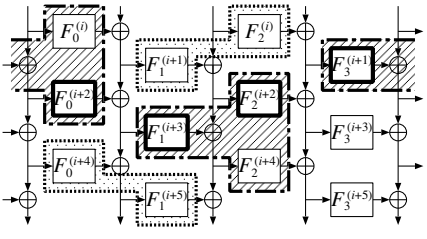

Fig. 11. Case 2-1-1

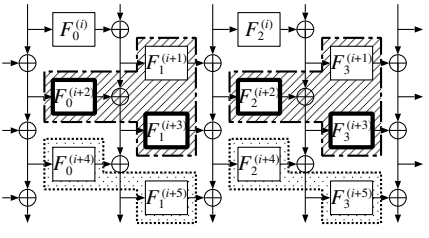

Fig. 12. Case 2-1-2

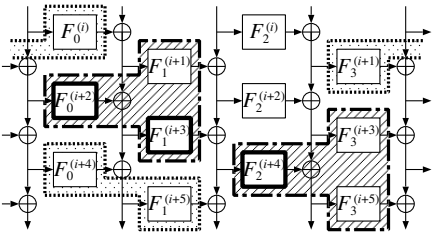

Fig. 13. Case 2-2