論文 / 著書情報
Article / Book Information

Title	On Generalizd Feistel Structures Using the Diffusion Switching Mechanism
Authors	Taizo Shirai, Kiyomichi Araki
出典 / Citation	IEICE Transaction on Fundamentals, Vol. E-91-A, No. 8, pp. 2120-2129
発行日 / Pub. date	2008, 8
URL	http://search.ieice.org/
権利情報 / Copyright	本著作物の著作権は電子情報通信学会に帰属します。 Copyright (c) 2008 Institute of Electronics, Information and Communication Engineers.

IEICE TRANS. FUNDAMENTALS, VOL.E91–A, NO.8 AUGUST 2008

PAPER

On Generalized Feistel Structures Using the Diffusion Switching Mechanism

Taizo SHIRAI[†a)], ***Member and*** **Kiyomichi ARAKI**[††b)], ***Fellow***

SUMMARY To design secure blockciphers, estimating immunity against differential attack and linear attack is essential. Recently, Diffusion Switching Mechanism (DSM) is proposed as a design framework to enhance the immunity of Feistel structure against differential attack and linear attack. In this paper, we give novel results on the effect of DSM on three generalized Feistel structures, i.e. Type-I, Type-II and Nyberg's structures. We first show a method for roughly estimating lower bounds of a number of active S-boxes in Type-I and Type-II structures using DSM. Then we propose an improved search algorithm to find lower bounds for generalized structures efficiently. Experimental results obtained by the improved algorithm show that DSM raises lower bounds for all of the structures, and also show that Nyberg's structure has the slowest diffusion effect among them when SP-type F-functions are used.

key words: *blockcipher, diffusion switching mechanism, generalized feistel structure*

1. Introduction

One of the established techniques of designing secure cryptographic primitives including blockciphers, streamciphers, and hash functions makes use of moderate sized non-linear functions, called S-boxes, and linear functions to propagate the non-linearity [1]–[5]. Especially in designing secure blockciphers, it is necessary to evaluate immunity of the cipher in terms of differential attack and linear attack which are known as general and powerful attacks for blockciphers [6], [7]. A practical approach known so far in evaluation of the immunity against these attacks is to estimate guaranteed numbers of active S-boxes [1], [4], [8], [9].

There are two types of approaches to show the guaranteed numbers of active S-boxes for an underlying structure. One shows a method for roughly estimating a lower bound with proofs. It is a useful tool to grasp the strength of structures. However it is sometimes valid for only limited numbers of rounds. The other approach shows lower bounds by search algorithms. The approach usually outputs detailed results which are useful for designing actual ciphers, but it needs considerable calculation cost to get the results for large parameter sets. To make use of both advantages, finding both results for the target structure are expected.

In the trend of the blockcipher design, the Feistel structure is one of the most popular and well-studied structures [2], [4], [10]. It is common that F-functions in the Feistel structure employ S-boxes, thus the matter of counting active S-boxes arises. The first theoretical research on finding the lower bounds of active S-boxes for Feistel structure was done by Kanda [8]. In his work, a method for roughly estimating a lower bound for Feistel structure with SP-type F-function are shown. Then Aoki et al. showed efficient search algorithm [4] which outputs tighter and detailed lower bounds for more rounds in the same structure. The algorithm is obtained by modifying Matsui's efficient differential path search algorithm [11].

Moreover, generalized Feistel structures which treat three or more data branches are known as alternative structures [12], [13]. Studies on these structures show that its flexibility of accepting both various sized data blocks and various sized F-functions is a desirable property to design practical ciphers [14]–[17]. Wu et al. studied the number of active S-boxes of generalized Feistel structure [18] in line with Kanda's result.

Recently, Shirai and Shibutani proposed a new property of the Feistel structure [19]. They showed that if each diffusion matrix in the SP-type F-function in conventional Feistel structure is chosen from two or more distinct matrices in a switching manner, the guaranteed number of active S-boxes become larger than the case of using a single matrix. The new design framework is called Diffusion Switching Mechanism (hereafter called DSM). The property is analyzed further in detail, a method for roughly estimating a lower bound is shown and reasonable search algorithms are proposed [20], [21]. Furthermore, a new blockcipher using one of the generalized Feistel structures adopting DSM was proposed [22]. However finding proofs for lower bounds and showing efficient search algorithms which can be applied to the generalized Feistel structures are still open.

In this paper we extend the above research to study effects of DSM on three representative generalized Feistel structures, which are known as Type-I, Type-II and Nyberg's structures [12], [13]. First, we show proofs of a method for roughly estimating a lower bound of Type-I and Type-II generalized Feistel structures using DSM. The results indicate that both structures have the same degree of increased estimated active S-boxes per F-function. Also, these results for both structures can be considered as natural extensions of known results for conventional Feistel structures.

Moreover, we propose an improved search algorithm to find tighter lower bounds for generalized structures by introducing an additional branch-cutting technique. Using

Manuscript received August 8, 2007.
Manuscript revised January 25, 2008.

[†]The author is with Sony Corporation, Tokyo, 141-0001 Japan.
[††]The author is with Tokyo Institute of Technology, Tokyo, 152-8550 Japan.
a) E-mail: Taizo.Shirai@jp.sony.com
b) E-mail: araki@mobile.ee.titech.ac.jp

DOI: 10.1093/ietfec/e91–a.8.2120

the improved algorithm three generalized structures including Nyberg's structure are compared in a quantitative manner. Experimental results for four branches cases reveal that DSM raise the lower bound for all of these structures, and also show that Nyberg's structure doesn't guarantee as many active S-boxes as Type-I and Type-II structures. We expect that the improved algorithm can be used for further analysis of the variety of generalized Feistel structures.

This paper is organized as follows: in Sect. 2, definitions for generalized Feistel structures are introduced. In Sect. 3, previous work on DSM is explained. Then we give proofs for a method for roughly estimating lower bounds of Type-I and Type-II structures in Sect. 4. Sect. 5 describes search algorithms and an improved technique, then evaluates three structures. Finally Sect. 6 concludes this paper.

2. Target Structures

In this paper, we treat several types of generalized Feistel structures. First of all, the definition of conventional Feistel structure with n-bit data block, where n is even, is introduced. Let P_0, P_1 be $n/2$-bit input words, let C_0, C_1 be $n/2$-bit output words, and $F_i(k, x)$ be a F-function of the i-th round which takes k as an $n/2$-bit round key and x as an $n/2$-bit input data. r denotes the number of total rounds. Then Feistel structure is defined as:

Step 1. $X_0 \leftarrow P_0,\ X_1 \leftarrow P_1$
Step 2. For $i = 1$ to r do the following:
 Step 2.1 $X_1 \leftarrow X_1 \oplus F_i(RK_i, X_0)$
 Step 2.2 $tmp \leftarrow X_1, X_1 \leftarrow X_0, X_0 \leftarrow tmp$
Step 3. $C_0 \leftarrow X_0,\ C_1 \leftarrow X_1$

In the above, RK_i $(1 \le i \le r)$ are provided by a key scheduling part which is not defined here. Without loss of generality, a swap operation at the final round is included.

Then three generalized Feistel structures which operate d data branches ($d \ge 2$) are shown. Here, we call a class of structures *generalized* Feistel if it is identical with the conventional Feistel structure in case of $d = 2$. Our targets in this study are "Type-I,""Type-II" and "Nyberg's" generalized Feistel structures. The first two structures are defined by Zheng et al. [12], and the last one is defined by Nyberg [13]. Several cryptographic properties of these generalized structures are studied in [15], [17]. Definitions of these generalized structures are given in this section.

Let n be the integer $d|n$ and $P_0, \ldots, P_{d-1}$ be n/d-bit plaintext words, and let $C_0, \ldots, C_{d-1}$ be n/d-bit ciphertext words. Then Type-I generalized Feistel structure is defined as:

Step 1. $X_0 \leftarrow P_0, \cdots, X_{d-1} \leftarrow P_{d-1}$
Step 2. For $i = 1$ to r do the following:
 Step 2.1 $X_1 \leftarrow X_1 \oplus F_i(RK_i, X_0)$
 Step 2.2 $tmp \leftarrow X_{d-1}$,
 $X_j \leftarrow X_{j-1}$ (for $j = d - 1$ to 1),
 $X_0 \leftarrow tmp$
Step 3. $C_0 \leftarrow X_0, \cdots, C_{d-1} \leftarrow X_{d-1}$

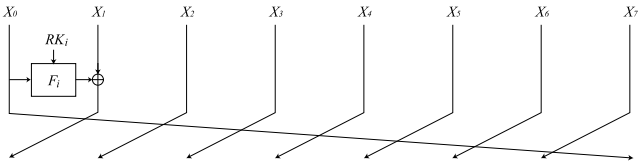

Fig. 1 A round function of Type-I Feistel structure. ($d = 8$)

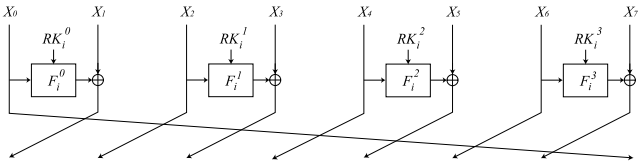

Fig. 2 A round function of Type-II Feistel structure. ($d = 8$)

Like conventional Feistel structure, Type-I structure calls a single F-function per round, and the permutation way of data branches is a rotation style. Figure 1 shows a round function of the Type-I structure in case of $d = 8$.

Type-II structure uses a plural numbers of F-function per round, and the number of branches d is even. Let $F_i^j(x, y)$ be the j-th F-function from the left in the i-th round. Type-II generalized Feistel structure is defined as follows.

Step 1. $X_0 \leftarrow P_0, \cdots, X_{d-1} \leftarrow P_{d-1}$
Step 2. For $i = 1$ to r do the following:
 Step 2.1 For $j = 0$ to $d/2 - 1$ do the following:
  Step 2.1.1 $X_{2j+1} \leftarrow X_{2j+1} \oplus F_i^j(RK_i^j, X_{2j})$
 Step 2.2 $tmp \leftarrow X_{d-1}$,
 $X_j \leftarrow X_{j-1}$ (for $j = d - 1$ to 1),
 $X_0 \leftarrow tmp$
Step 3. $C_0 \leftarrow X_0, \cdots, C_{d-1} \leftarrow X_{d-1}$

The difference between Type-I and Type-II structures is the number of F-functions per round, i.e. $d/2$ F-functions are called in Type-II. Figure 2 shows a round function of the Type-II structure in case of $d = 8$.

Lastly, using the same notion of F-functions for Type-II, Nyberg's generalized Feistel structure is defined as follows[†].

Step 1. $X_0 \leftarrow P_0, \cdots, X_{d-1} \leftarrow P_{d-1}$
Step 2. For $i = 1$ to r do the following:
 Step 2.1 For $j = 0$ to $d/2 - 1$ do the following:
  Step 2.1.1 $X_{2j+1} \leftarrow X_{2j+1} \oplus F_i^j(RK_i^j, X_{2j})$
 Step 2.2 $tmp \leftarrow X_1$,
 $X_{2j+1} \leftarrow X_{2j+3}$ (for $j = 0$ to $d/2 - 2$)
 $X_{d-1} \leftarrow X_{d-2}$
 $X_{2j} \leftarrow X_{2j-2}$ (for $j = d/2 - 1$ to 1)
 $X_0 \leftarrow tmp$
Step 3. $C_0 \leftarrow X_0, \cdots, C_{d-1} \leftarrow X_{d-1}$

The difference between Type-II and Nyberg's is the

[†]Though several expressions are possible according to the positions and the directions of F-functions, we follow the definition by Kim et al. [17].

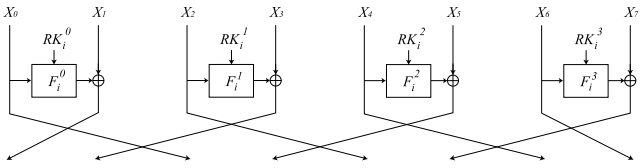

Fig. 3 A round function of Nyberg's Feistel structure. ($d = 8$)

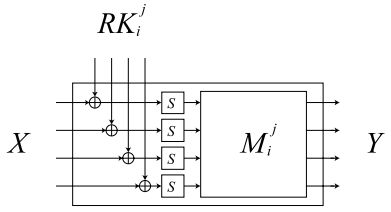

Fig. 4 F-function F_j^i.

permutation way of data branches. Nyberg's structure employs a symmetric and a more complex style. Figure 3 shows a round function of Nyberg's structure in case of $d = 8$.

In this paper, we assume that the type of F-functions used in these structures is the SP-type F-function which is one of the popular F-functions [8]. Let l be the size of S-boxes and let m be the dimension of a diffusion matrix, then an SP-type F-function taking an lm-bit round key RK, input data X and output data Y is defined as:

Step 1. $T \leftarrow RK \oplus X$
Step 2. Let $T = T_0 \mid T_1 \mid \cdots \mid T_{m-1},\ T_i \in \{0,1\}^l$
$T_i \leftarrow S(T_i)$ (for $i = 0$ to $m-1$)
Step 3. Let $Y = Y_0 \mid Y_1 \mid \cdots \mid Y_{m-1},\ Y_i \in \{0,1\}^l$
${}^t(Y_0, Y_1, \cdots, Y_{m-1}) = M\ {}^t(T_0, T_1, \cdots, T_{m-1})$

where $A|B$ denotes a concatenation of data A and B. $S(\cdot)$ denotes an l-bit bijective S-box and M denotes an non-singular $m \times m$ matrix over a chosen field GF(2^l). Hereafter M_i and M_i^j denotes diffusion matrices M used in F-functions F_i and F_i^j in generalized Feistel structures, respectively. Figure 4 shows an example of a SP-type F-function F_i^j in case of $m = 4$.

Using the above definitions, the block length n is now determined by three parameters d, l and m. For example, a typical block length $n = 128$ is obtained by any choice of $(d, l, m) = (2, 8, 8)$, $(4, 8, 4)$ or $(8, 4, 4)$.

3. Previous Work

Recently it is shown that if two or more distinct diffusion matrices are used in conventional Feistel structure in a switching manner, the guaranteed number of active S-boxes is increased from that of a single matrix case [19]–[21]. The design approach is called Diffusion Switching Mechanism (DSM). To begin with, we give some definitions to review the DSM.

Definition 1 (Bundle Weight): Let p and l be positive integers, and let $x \in \{0,1\}^{pl}$ be a bit string also represented as a vector $\boldsymbol{x} = (x_0, x_1, \ldots, x_{p-1}) \in \{\{0,1\}^l\}^p$ where $x_i \in \{0,1\}^l$, then the bundle weight $w_l(x)$ is defined as $w_l(x) = \#\{i \mid 0 \le i \le p-1, x_i \neq 0^l\}$, where $\#\boldsymbol{S}$ denotes a number of elements in the set $\boldsymbol{S}$.

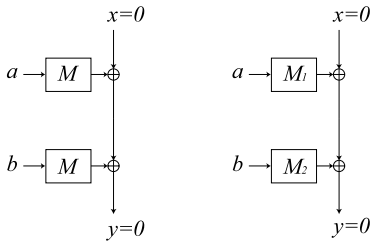

Fig. 5 Concept of DSM.

Definition 2 (Branch Number): Let p, q and l be positive integers, and let $P : \{\{0,1\}^l\}^p \rightarrow \{\{0,1\}^l\}^q$ be a mapping. Then a branch number of P is defined as $\mathcal{B}_l(P) = \min_{\boldsymbol{a} \neq \boldsymbol{0}, \boldsymbol{a} \in \{\{0,1\}^l\}^p} \{w_l(\boldsymbol{a}) + w_l(P(\boldsymbol{a}))\}$.

Basic concept of DSM is explained using Fig. 5. Let M be a non-singular $m \times m$ matrix, and $\boldsymbol{a}, \boldsymbol{b} \in \{\{0,1\}^l\}^m$ are m-dimensional vectors. The left side of Fig. 5 shows that the two output vectors through the same matrix M are XORed to the data line. Suppose that x and y are fixed for 0, what is the possible smallest sum of bundle weights of $w_l(\boldsymbol{a}) + w_l(\boldsymbol{b})$? In this case it is shown that $w_l(\boldsymbol{a}) + w_l(\boldsymbol{b}) = 2$ is a possible value because $M(\boldsymbol{a} + \boldsymbol{b}) = \boldsymbol{0}$ is realized by $\boldsymbol{a} = \boldsymbol{b}, w_l(\boldsymbol{a}) = 1$ for any fixed M. However, if two different matrices M_1 and M_2 are used as in the right side of Fig 5, then $w_l(\boldsymbol{a}) + w_l(\boldsymbol{b}) \ge \mathcal{B}_l([M_1|M_2])$, where $[A|B]$ denotes an $m \times 2m$ matrix obtained by concatenating matrices A and B. From Def. 2, $\mathcal{B}_l([M_1|M_2])$ can be $m + 1$ at most, which is optimal diffusion [1], [21]. If we put S-boxes just before the matrices as an SP-type F-function, $w(\boldsymbol{a}) + w(\boldsymbol{b})$ is regarded as the number of active S-boxes in this case. From this observation, the latter construction can guarantee larger number of active S-boxes if the above conditions are satisfied. DSM incorporates this property in the whole Feistel structure to raise the lower bounds.

Then we give definitions of B_1^D, B_2^D and B_2^L to show the guaranteed number of differential active S-boxes for conventional Feistel structure.

Definition 3:

$$B_1^D = \min_{1 \le i \le r} (\mathcal{B}_l(M_i)),$$

$$B_2^D = \min_{1 \le i \le r-2} (\mathcal{B}_l([M_i|M_{i+2}])).$$

$$B_2^L = \min_{1 \le i \le r-2} (\mathcal{B}_l([{}^tM_i^{-1}|{}^tM_{i+2}^{-1}])).$$

Note that $B_1^D \ge B_2^D$ because $\mathcal{B}_l(A) \ge \mathcal{B}_l(A|B)$ for any matrices A and B. Using these definitions[†], the following theorem is obtained [20], [21].

[†] B_3^D is also defined in [21], but we focus on two matrices relation in this study.

Theorem 1: Any 6 consecutive rounds in the Feistel structure using SP-type F-functions guarantee at least $B_1^D + B_2^D$ differential active S-boxes and $2B_2^L$ linear active S-boxes.

Theorem 1 suggests a new design approach of Feistel cipher. Consider designing a Feistel structure where $l = 8$, $m = 8$, which treats a 128-bit block, then choose two matrices A and B which satisfy $\mathcal{B}_l(A) = 9, \mathcal{B}_l(B) = 9$, $\mathcal{B}_l([A|B]) = 9$ and $\mathcal{B}_l([{}^tA^{-1}|{}^tB^{-1}]) = 9$, i.e. A and B keep an optimal branch number† with additional branch number conditions. Then A and B are set as $M_i = A$ where $i \mod 4 = 0$ or 1, and $M_i = B$ where $i \mod 4 = 2$ or 3. This setting results in $B_1^D = B_2^D = B_2^L = 9$, and the theorem immediately implies that any consecutive 6 rounds, 12 rounds, ..., 6R rounds of the designed Feistel structure guarantee at least 18, 36, ..., 18R differential and linear active S-boxes, respectively. Because the diffusion matrices are used in switching manner, the design is called *Diffusion Switching Mechanism*.

A series of works on DSM opened a new design approach of Feistel structure, but no theoretical results on generalized Feistel structures which use DSM were reported so far. We study this issue, and several novel results of lower bound of generalized structures are shown.

4. Lower Bounds of Type-I and Type-II Generalized Feistel Structures

In this section proofs for a method for roughly estimating lower bounds for Type-I and Type-II generalized Feistel structures are shown. Then we discuss these results by comparing the obtained bounds for both structures.

4.1 Type-I Generalized Feistel Structure Using DSM

First, the DSM for conventional Feistel structure is transformed for Type-I generalized Feistel structure. Recall that in conventional Feistel structure, the relations of two matrices M_i in F_i and M_{i+2} in F_{i+2} for all i play important roles because the output of these two matrices are XORed to the same data branch. Figure 6 shows the relationship between these F-functions explicitly by using an untwisted style Feistel structure in which each data branch is represented as a vertical line.

Also, Type-I generalized Feistel structure can be illustrated as an untwisted form as in Fig. 7. The figure shows that the relations of two matrices between M_i in F_i and M_{i+d} in F_{i+d} for all i should be taken into account.

Therefore, the definitions of B_1^D, B_2^D and B_2^L are modified as follows.

Definition 4:

$$ {}^{\mathrm{I}}B_1^D = \min_{1\le i\le r}(\mathcal{B}_l(M_i)), $$

$$ {}^{\mathrm{I}}B_2^D = \min_{1\le i\le r-d}(\mathcal{B}_l([M_i|M_{i+d}])). $$

$$ {}^{\mathrm{I}}B_2^L = \min_{1\le i\le r-d}(\mathcal{B}_l([{}^tM_i^{-1}|{}^tM_{i+d}^{-1}])). $$

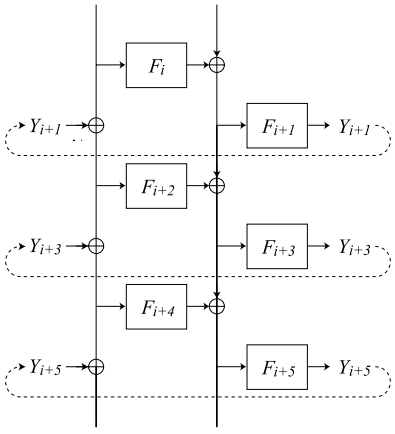

Fig. 6 Feistel structure. (Untwisted form)

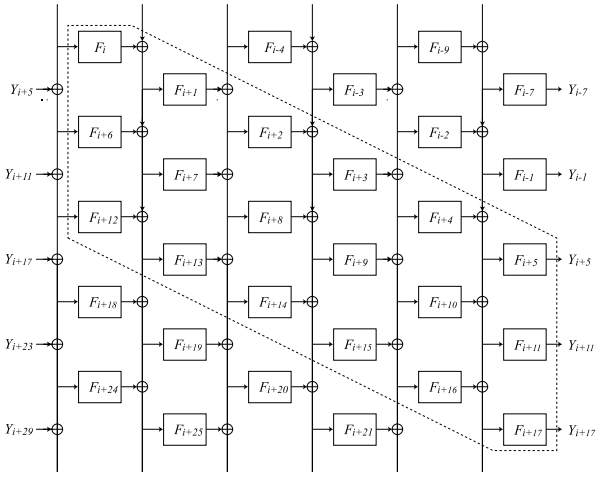

Fig. 7 Type-I generalized feistel structure. ($d = 6$, Untwisted)

The above definition directly implies ${}^{\mathrm{I}}B_1^D \ge {}^{\mathrm{I}}B_2^D$.

Using this definitions, proven lower bound of differential and linear active S-boxes for Type-I structure are shown in the following sections.

4.1.1 Differential Active S-Boxes in Type-I Structure

Recall that X_i and RK_i are an input and a round-key of i-th F-function F_i, respectively. Moreover we let D_i be the number of differential active S-boxes of F_i, where $D_i = w_l(\Delta X_i)$, ΔX_i denotes a difference of X_i. If non-zero difference is input to Type-I generalized Feistel structure, the following properties hold:

Property 1: There is at least one F-function which has at least one active S-box in any consecutive d rounds, because the invertibility of the structure assures the property.

Property 2: If $D_i = 0$, then $D_{i-d+1} = D_{i+1}$, and if $D_i \neq 0$, then $D_{i-d+1} + D_i + D_{i+1} \ge {}^{\mathrm{I}}B_1^D$. This is implied by the equation $F_i(RK_i, X_i) = X_{i-d-1} \oplus X_{i+1}$.

†Also known as MDS matrices because it can be obtained from the maximum distance separable (MDS) codes [23].

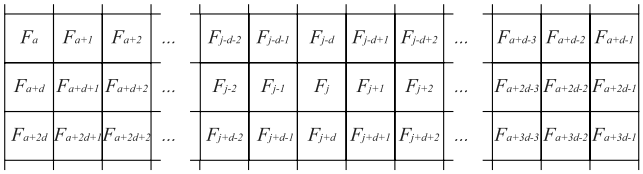

Fig. 8 $3d$ rounds of Type-I structure. (3-layer form)

Property 3: If $D_i \neq 0$ or $D_{i+d} \neq 0$, then $D_{i-d+1}+D_i+D_{i+d}+D_{i+d+1} \geq {}^{\mathrm{I}}B_2^D$. This is implied by the equation $F_i(K_i, X_i) \oplus F_{i+d}(K_{i+d}, X_{i+d}) = X_{i-d+1} \oplus X_{i+d+1}$.

These properties are also explained in [21]. Using the above properties, we obtain the following theorem.

Theorem 2: Let $d \geq 3$. Any consecutive $3d$ rounds of d-branch Type-I generalized Feistel structure using SP-type F-functions guarantee ${}^{\mathrm{I}}B_1^D + {}^{\mathrm{I}}B_2^D$ differential active S-boxes.

Proof: We consider that a consecutive $3d$ rounds which starts from the a-th round, and the $3d$ consecutive rounds are regarded as a three-layer form in which one layer contain d consecutive rounds. Each layer starts from the $a, a+d$ and $a+2d$-th rounds. Figure 8 shows this three-layer form, and the region boxed by a dashed line in Fig. 7 shows the three layers from i-th round for $d = 6$ case.

Property 1 guarantees at least one F-function which has a non-zero difference in the 2nd layer. According to the positions where non-zero differences exist in the 2nd layer, two cases are separately considered in the following.

CASE 1 (A difference exist in the 2nd layer except the both ends, i.e. $D_{a+d} = D_{a+2d-1} = 0$.)
Pick a non-zero difference in the 2nd-layer, and let it be D_j $(a+d < j < a+2d-1)$. Then Property 2 and 3 imply,

$$D_{j-d+1} + D_j + D_{j+1} \geq {}^{\mathrm{I}}B_1^D, \quad (1)$$

$$D_{j-d+1} + D_j + D_{j+d} + D_{j+d+1} \geq {}^{\mathrm{I}}B_2^D. \quad (2)$$

In this case, the following three cases are considered:

1A If $D_{j+d-1} \neq 0$, then Prop. 3 implies $D_{j-d} + D_{j-1} + D_{j+d-1} + D_{j+d} \geq {}^{\mathrm{I}}B_2^D$. By simply combining this and (1) we get $\sum_{i=a}^{a+3d-1} D_i \geq {}^{\mathrm{I}}B_1^D + {}^{\mathrm{I}}B_2^D$ in this case.

1B If $D_{j+1} \neq 0$, then Prop. 2 implies $D_{j-d+2}+D_{j+1}+D_{j+2} \geq {}^{\mathrm{I}}B_1^D$. By combining it and (1) we get $\sum_{i=a}^{a+3d-1} D_i \geq 2 \times {}^{\mathrm{I}}B_1^D$ in this case.

1C If $D_{j+d-1} = D_{j+1} = 0$, then the condition of $D_{j+d-1} = 0$ and Prop. 2 imply $D_{j+d} = D_j \neq 0$. Then $D_{j+d} \neq 0$ and Prop. 2 imply

$$D_{j+1} + D_{j+d} + D_{j+d+1} \geq {}^{\mathrm{I}}B_1^D. \quad (3)$$

Eq. (1) and (3) have an overlapping term D_{j+1}, but we now know $D_{j+1} = 0$. As a result, we obtain $\sum_{i=a}^{a+3d-1} D_i \geq 2 \times {}^{\mathrm{I}}B_1^D$.

CASE 2 (A non-zero difference only exist at either of both of the edges in the 2nd layer, i.e. $D_j = 0$ $(a+d+1 \leq j \leq a+2d-2)$.)
In this situation, the following three cases are considered:

2A If $D_{a+d} \neq 0$ and $D_{a+2d-1} = 0$, then Prop. 2 gives $D_{a+2d} = D_{a+d} \neq 0$. Moreover, Prop. 2 gives $D_{a+1} + D_{a+d} + D_{a+d+1} \geq {}^{\mathrm{I}}B_1^D$ and $D_{a+d+1} + D_{a+2d} + D_{a+2d+1} \geq {}^{\mathrm{I}}B_1^D$. There is an overlapping term D_{a+d+1}, but we assumed $D_{a+d+1} = 0$. Thus we obtain $\sum_{i=a}^{a+3d-1} D_i \geq 2 \times {}^{\mathrm{I}}B_1^D$ in this case.

2B If $D_{a+d} = 0$ and $D_{a+2d-1} \neq 0$. Since $D_{a+2d-2} = 0$, Prop. 2 gives $D_{a+d-1} = D_{a+2d-1} \neq 0$. Thus, Prop. 2 gives $D_a + D_{a+d-1} + D_{a+d} \geq {}^{\mathrm{I}}B_1^D$. Also $D_{a+2d-1} \neq 0$ gives $D_{a+d} + D_{a+2d-1} + D_{a+2d} \geq {}^{\mathrm{I}}B_1^D$. There is an overlapping term D_{a+d} in these inequalities, but we assumed $D_{a+d} = 0$. Thus we obtain $\sum_{i=a}^{a+3d-1} D_i \geq 2 \times {}^{\mathrm{I}}B_1^D$ in this case.

2C If $D_{a+d} \neq 0$ and $D_{a+2d-1} \neq 0$, then the condition of $D_{a+d} \neq 0$ and Prop. 2 imply $D_{a+1}+D_{a+d}+D_{a+d+1} \geq {}^{\mathrm{I}}B_2^D$. Moreover, D_{a+2d-1} and Prop. 3 imply $D_a + D_{a+d-1} + D_{a+2d-1} + D_{a+2d} \geq {}^{\mathrm{I}}B_2^D$. As a result we obtain $\sum_{i=k}^{k+3n-1} D_i \geq {}^{\mathrm{I}}B_1^D + {}^{\mathrm{I}}B_2^D$.

Combining all cases, we conclude that at least ${}^{\mathrm{I}}B_1^D + {}^{\mathrm{I}}B_2^D$ differential active S-boxes are guaranteed in $3d$ rounds of Type-I structure. □

4.1.2 Linear Active S-Boxes in Type-I Structure

Similar to the differential case, we write a number of linear active S-boxes for the i-th round as L_i. Let ΓX_i and ΓY_i be linear masks for input and output of F_i, respectively. If a non-zero linear mask is input to Type-I generalized Feistel structure, the following properties hold.

Property 4: There is at least one F-function which has at least one linear active S-box in any consecutive d rounds due to the invertibility of the structure.

Property 5: For any set of L_i, L_{i+1} and L_{i+d} satisfy:

- $L_i = L_{i+1} = L_{i+d} = 0$, or
- $L_i+L_{i+1}+L_{i+d} \geq {}^{\mathrm{I}}B_2^L$, where two of the terms are always non-zero.

This is implied by the equation $\Gamma X_{i+1} = \Gamma Y_i \oplus \Gamma Y_{i+d}$.

Using the above properties, we obtain,

Theorem 3: Let $d \geq 3$. Any consecutive $3d$ rounds of d-branch Type-I generalized Feistel structure using SP-type F-functions guarantee at least $2 \times {}^{\mathrm{I}}B_2^L$ linear active S-boxes.

Proof: Similar to the proof of Theorem 2, we show a guaranteed number of active S-boxes in consecutive $3d$ rounds which starts from the a-th round.
CASE 1 (One or more non-zero linear mask exist in the second layer except the left end, i.e. $L_j \neq 0$ $(a+d+1 \leq j \leq a+2d-1)$.)
Then Prop. 5 implies:

$$L_{j-1} + L_j + L_{j+d-1} \geq {}^{\mathrm{I}}B_2^L, \quad (4)$$

$$L_j + L_{j+1} + L_{j+d} \geq {}^{\mathrm{I}}B_2^L. \quad (5)$$

In this situation, the following two cases are considered:

1A If $L_{j-d} \neq 0$ or $L_{j-1} \neq 0$, these conditions imply $L_{j-d-1} + L_{j-d} + L_{j-1} \geq {}^{\mathrm{I}}B_2^L$ which do not contain any overlapped term with (5). As a result we obtain $\sum_{i=k}^{k+3n-1} L_i \geq 2 \times {}^{\mathrm{I}}B_2^L$.

1B If $L_{j-d} = L_{j-1} = 0$, from Prop. 5, $L_j \neq 0$ and $L_{j-d} = 0$ imply $L_{j-d+1} \neq 0$. Then L_{j-d+1} gives

$$L_{j-d+1} + L_{j-d+2} + L_{j+1} \geq {}^{\mathrm{I}}B_2^L. \tag{6}$$

If $d \geq 4$, (4) and (6) give $\sum_{i=k}^{k+3n-1} L_i \geq 2 \times {}^{\mathrm{I}}B_2^L$. If $d = 3$, L_{j-1} in (4) and L_{j-d+2} in (6) overlap. But we assumed $L_{j-1} = 0$, thus they also give $\sum_{i=k}^{k+3n-1} L_i \geq 2 \times {}^{\mathrm{I}}B_2^L$.

CASE 2 (A non-zero linear mask is found only at the left end of the second layer, i.e., $L_{a+d} \neq 0$, $L_i = 0$ $(a + d + 1 \leq j \leq a + 2d - 1)$.)
Then Prop. 5 implies

$$L_{a+d-1} + L_{a+d} + L_{a+2d-1} \geq {}^{\mathrm{I}}B_2^L, \tag{7}$$

$$L_{a+d} + L_{a+d+1} + L_{a+2d} \geq {}^{\mathrm{I}}B_2^L. \tag{8}$$

Since $L_{a+2d-1} = 0$, (7) gives $L_{a+d-1} \neq 0$. Then $L_{a+d-1} \neq 0$ implies

$$L_{a+d-2} + L_{a+d-1} + L_{a+2d-2} \geq {}^{\mathrm{I}}B_2^L. \tag{9}$$

If $d \geq 4$, (8) and (9) give $\sum_{i=k}^{k+3n-1} L_i \geq 2 \times {}^{\mathrm{I}}B_2^L$. If $d = 3$, L_{a+d+1} in (8) and L_{a+2d-2} in (9) overlap. But we assumed $L_{a+4} = 0$, then they also give $\sum_{i=k}^{k+3n-1} L_i \geq 2 \times {}^{\mathrm{I}}B_2^L$.

Combining all cases, we conclude that at least ${}^{\mathrm{I}}B_2^L$ linear active S-boxes are guaranteed in $3d$ consecutive rounds of Type-I structure. □

4.2 Type-II Generalized Feistel Structure Using DSM

Next, the DSM is applied to Type-II generalized Feistel structure. Type-II structure where $d = 6$ is illustrated as an untwisted form as in Fig. 9. To use the DSM, two matrices between M_i^j in F_i^j and M_{i+2}^{j-1} in F_{i+2}^{j-1} for all possible i and j should satisfy the DSM branch number conditions. Note that the indices at the upper right of M and F are taken mod $d/2$, i.e. $d/2 = 0$, and $-1 = d/2 - 1$.

According to the above observation, the definitions of B_1^D, B_2^D and B_2^L are modified as follows:

Definition 5:

$${}^{\mathrm{II}}B_1^D = \min_{1 \leq i \leq r,\ 0 \leq j < d/2} (\mathcal{B}_l(M_i^j)),$$

$${}^{\mathrm{II}}B_2^D = \min_{1 \leq i \leq r-2,\ 0 \leq j < d/2} (\mathcal{B}_l([M_i^j \mid M_{i+2}^{j-1}]),$$

$${}^{\mathrm{II}}B_2^L = \min_{1 \leq i \leq r-2,\ 0 \leq j < d/2} (\mathcal{B}_l([{}^t(M_i^j)^{-1} \mid {}^t(M_{i+2}^{j-1})^{-1}])).$$

The above definition directly implies ${}^{\mathrm{II}}B_1^D \geq {}^{\mathrm{II}}B_2^D$.

Using these definitions, proven lower bound of differential and linear active S-boxes for Type-II structure are shown in the following:

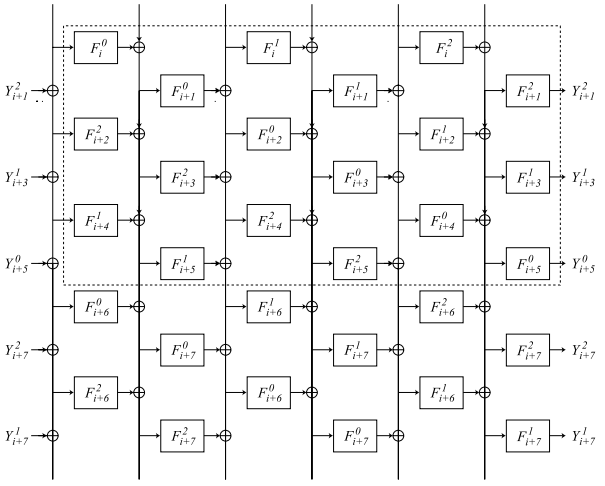

Fig. 9 Type-II generalized Feistel structure. ($d = 6$, Untwisted)

4.2.1 Differential Active S-Boxes in Type-II Structure

Let X_i^j, K_i^j and D_i^j be an input, a round-key and a number of differential active S-boxes in F_i^j, respectively. If non-zero difference is input to Type-II generalized Feistel structure, we can use the following properties:

Property 6: There is at least one F-function which contains at least one active S-box in any consecutive 2 rounds due to the invertibility of the structure.

Property 7: If $D_i^j = 0$, then $D_{i-1}^{j+1} = D_{i+1}^j$, and if $D_i^j \neq 0$, then $D_i^j + D_{i-1}^{j+1} + D_{i+1}^j \geq {}^{\mathrm{II}}B_1^D$. This is implied by the equation $F_i^j(K_i^j, X_i^j) = X_{i-1}^{j+1} \oplus X_{i+1}^j$.

Property 8: If $D_i^j \neq 0$ or $D_{i+2}^{j-1} \neq 0$, then $D_i^j + D_{i+2}^{j-1} + D_{i-1}^{j+1} + D_{i+3}^{j-1} \geq {}^{\mathrm{II}}B_2^D$. This is implied by the equation $F_i^j(K_i^j, X_i^j) \oplus F_{i+2}^{j-1}(K_{i+2}^{j-1}, X_{i+2}^{j-1}) = X_{i-1}^{j+1} \oplus X_{i+3}^{j-1}$.

Using these properties, we obtain

Theorem 4: Let $d \geq 4$. Any consecutive 6 rounds of d-branch Type-II generalized Feistel Structure using SP-type F-functions guarantee ${}^{\mathrm{II}}B_1^D + {}^{\mathrm{II}}B_2^D$ differential active S-boxes.

Proof: We consider 6 consecutive rounds that starts from the a-th round. To make the proof easy to understand, we put $3d$ F-functions in the 6 rounds into alternatively arranged boxes as in Figure 10. The width of the boxes is d. F-functions in the same round are found in the boxes in the same row, and F-functions in the next rounds are found in the next columns. The region boxed by a dashed line in Fig. 9 shows the 6 rounds from i-th round for $d = 4$ case.

Prop. 6 guarantees at least one F-function which has a non-zero difference in the 3rd or 4th rounds, i.e. $(a + 2)$-th round or $(a + 3)$-th round.
CASE 1 (Any non-zero difference exists in the 3rd round, i.e. $D_{a+2}^j \neq 0$.)
Then Prop. 7 and 8 imply,

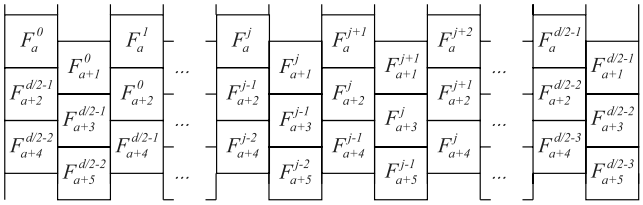

Fig. 10 Type-II generalized Feistel structure. (Box form)

$$D^j_{a+2} + D^{j+1}_{a+1} + D^j_{a+3} \geq {}^{\mathrm{II}}B^D_1, \tag{10}$$

$$D^j_{a+2} + D^{j-1}_{a+4} + D^{j+1}_{a+1} + D^{j-1}_{a+5} \geq {}^{\mathrm{II}}B^D_2. \tag{11}$$

1A If $D^{j-1}_{a+3} \neq 0$, then Prop. 8 implies $D^j_{a+1} + D^{j-1}_{a+3} + D^{j+1}_a + D^{j-1}_{a+4} \geq {}^{\mathrm{II}}B^D_2$. By combining it and (10), we obtain $\sum_{i=a}^{a+5}\sum_{j=0}^{d/2-1} D^j_i \geq {}^{\mathrm{II}}B^D_1 + {}^{\mathrm{II}}B^D_2$.

1B If $D^j_{a+3} \neq 0$, then Prop. 7 implies $D^j_{a+3} + D^{j+1}_{a+2} + D^j_{a+4} \geq {}^{\mathrm{II}}B^D_1$. By combining (11), we obtain $\sum_{i=a}^{a+5}\sum_{j=0}^{d/2-1} D^j_i \geq {}^{\mathrm{II}}B^D_1 + {}^{\mathrm{II}}B^D_2$.

1C If $D^{j-1}_{a+3} = D^j_{a+3} = 0$, then the condition of $D^{j-1}_{a+3} = 0$ and Prop. 7 imply $D^{j-1}_{a+4} = D^j_{a+2} \neq 0$. Using the Prop. 7 for D^j_{a+4}, we obtain

$$D^{j-1}_{a+4} + D^j_{a+3} + D^{j-1}_{a+5} \geq {}^{\mathrm{II}}B^D_1. \tag{12}$$

Eqs. (10) and (12) have an overlapping term D^j_{a+3}, but we assumed $D^j_{a+3} = 0$. As a result, we obtain $\sum_{i=a}^{a+5}\sum_{j=0}^{d/2-1} D^j_i \geq 2 \times {}^{\mathrm{II}}B^D_1 \geq {}^{\mathrm{II}}B^D_1 + {}^{\mathrm{II}}B^D_2$.

CASE 2 (Any non-zero difference exists in the 4th round.)
We can prove the same lowerbounds for this case as CASE 1 due to the symmetry of the structure. □

4.2.2 Linear Active S-Boxes in Type-II Structure

Similar to the differential case, we write a number of linear active S-boxes for F^j_i as L^j_i. If a non-zero linear mask is input to Type-II generalized Feistel structure, we can use the following properties:

Property 9: There is at least one F-function which contains at least one linear active S-box in any consecutive 2 rounds due to the invertibility of the structure.

Property 10: For any set of L^j_i, L^j_{i+1} and L^{j-1}_{i+2} satisfy:

- $L^j_i = L^j_{i+1} = L^{j-1}_{i+2} = 0$, or
- $L^j_i + L^j_{i+1} + L^{j-1}_{i+2} \geq {}^{\mathrm{II}}B^L_2$, where two of the terms are always non-zero.

Using the above properties, we show the following theorem.

Theorem 5: Let $d \geq 4$. Any consecutive 6 rounds of d-branch Type-II generalized Feistel structure using SP-type F-functions guarantee at least $2 \times {}^{\mathrm{II}}B^L_2$ linear active S-boxes.

Proof: Similar to Theorem 4, we prove that a guaranteed number of active S-boxes in 6 consecutive rounds which starts from the a-th round.
Prop. 9 guarantees at least one F-function which has non-zero linear mask in the 3rd or 4th rounds, i.e. $(a + 2)$-th round or $(a + 3)$-th round.
CASE 1 (Any non-zero linear mask exists in the 3rd round, i.e. $L^j_{a+2} \neq 0$.)
From Prop. 10, we obtain $L^j_{a+1} + L^j_{a+2} + L^{j-1}_{a+3} \geq {}^{\mathrm{II}}B^L_2$. Assume that each term in the inequality is non-zero, we can say

- $L^j_a + \boldsymbol{L^j_{a+1}} + L^{j-1}_{a+2} \geq {}^{\mathrm{II}}B^L_2$
- $L^{j+1}_a + L^{j+1}_{a+1} + \boldsymbol{L^j_{a+2}} \geq {}^{\mathrm{II}}B^L_2$
- $\boldsymbol{L^{j-1}_{a+3}} + L^{j-1}_{a+4} + L^{j-2}_{a+5} \geq {}^{\mathrm{II}}B^L_2$

Note that these three terms under consideration are emphasized in a bold type, and there is no overlapped term in the above three inequalities. Prop. 10 implies that at least two of the three terms are non-zero, therefore two of the above inequalities are valid. As a result, we obtain $\sum_{i=a}^{a+5}\sum_{j=0}^{d/2-1} L^j_i \geq 2 \times {}^{\mathrm{II}}B^L_2$
CASE 2 (Any non-zero linear mask exists in the 4th round.)
Similarly, we can prove the same lower bounds for this case as CASE 1 due to the symmetry of the structure. □

4.3 Discussion

The lower bounds shown in this section can be used as useful tools to measure strength of designed primitives using either generalized structure. Especially, due to the fact that Theorem 2 and 3 for Type-I structure are valid for $d \geq 3$ and Theorem 4 and 5 for Type-II structure are valid for $d \geq 4$, these results can be regarded as natural extensions of the results for conventional Feistel structure where $d = 2$ [21]. Moreover, the theorems imply that Type-I and Type-II structures guarantee the same degree of immunity per F-function against differential attack and linear attack when using DSM. Thus these results do not imply explicit superiority or inferiority between these structures with regard to the number of guaranteed active S-boxes per F-function.

5. Computational Evaluation

In this section we show the other approach to show lower bounds of generalized Feistel structures. We improve a known search algorithm to fit to generalized Feistel structures [19]. Then we compare the three generalized Feistel structures using guaranteed numbers of active S-boxes obtained by the improved search algorithm.

5.1 Basic Search Algorithm

The basic search algorithm counting active S-boxes is introduced in [19]. First, we explain the basic concept of the algorithm for Type-I generalized structure as an example. To find lower bounds for r-round Type-I Feistel structure,

1. For each candidate in all possible combinations of

Table 1 Basic search algorithm.

INPUT: R (a number of rounds), $\mathcal{ST}_R$ (target structure)
OUTPUT: a guaranteed number of active S-boxes for $\mathcal{ST}_R$

Main:
Step 1. Set global variable $LB = \infty$
Step 2. Call $Func(1)$
Step 3. Output LB

$Func(x)$
Step 4. If $x = NF_R + 1$ do the following:
If $LB > \sum_{p=1}^{NF_R} \mathcal{D}_p$, $LB \leftarrow \sum_{p=1}^{NF_R} \mathcal{D}_p$.
Step 5. If $x \neq NF_R + 1$. For $j = 0$ to m do the following:
Set $\mathcal{D}_x = j$ and check whether all properties
for the target structure are satisfied or not.
If check is OK, call $Func(x + 1)$

weight values D_i (or L_i), $(0 \leq D_i \leq m,\ 1 \leq i \leq r)$ do:

- Check inconsistency between given D_is (or L_is) determined by branch number conditions. If they are inconsistent, discard the candidate, else calculate and store a sum of D_is $(1 \leq i \leq r)$.

2. Output the smallest sum value as the lower bound of the target structure.

Properties shown in Sect. 4.1 are used to rule out wrong combinations of weight values. For example, in the properties of Type-I Feistel structure, letting ${}^1B_2^D = 5$ and $D_i \neq 0$, then the case of $D_{i-d+1} + D_i + D_{i+1} < 5$ is always judged as wrong for any i.

An actual search algorithm is a little sophisticated and is as follows. Let $\mathcal{ST}_R$ be an R-round generalized structure to be evaluated, and NF_i be a total number of F-functions in the first i rounds of $\mathcal{ST}_R$. Then we define alias names of F-functions $\mathcal{F}_1, \mathcal{F}_2, \cdots, \mathcal{F}_{NF_R}$ as $\mathcal{F}_i = F_i$ in Type-I generalized Feistel structure, and $\mathcal{F}_{di+j} = F_i^j$ for Type-II and Nyberg's generalized Feistel structures. Moreover, $\mathcal{D}_i$ and $\mathcal{L}_i$ denote numbers of differential and linear active S-boxes for $\mathcal{F}_i$, respectively. The basic algorithm to find the lower bounds of active S-boxes is defined as in Table 1.

In the above $Func(x)$ is a recursive function call. In Step 5. the properties for checking the consistency of D_is should be appropriately selected according to the type of structures described in the previous sections. To find lower bounds of linear active S-boxes, $\mathcal{D}_i$ is replaced with $\mathcal{L}_i$, and applied properties are changed for linear masks.

We confirmed that this algorithm works well for only small sized parameters. Our experimental result shows that even searching for 16-round Type-I Feistel structures $m = 4$, $d = 4$ requires more than one day. This huge calculation cost may sometimes be an obstacle to estimate the wide range of generalized Feistel structures.

5.2 Improved Search Algorithm

We speed up the basic algorithm by introducing an additional branch cutting technique. The improved algorithm is shown in Table 2. The major difference between the basic and the improved algorithms is that the improved algorithm makes the most of the information of lower bounds for smaller rounds. The idea of using information of smaller rounds is proposed by Matsui [11], but we used the idea in a different manner.

Table 2 Improved search algorithm.

INPUT: R (a number of rounds), $\mathcal{ST}_R$ (target structure)
OUTPUT: a guaranteed number of active S-boxes for $\mathcal{ST}_R$

Main:
Step 1. Set global variable $LB_i = \infty$ $(1 \leq i \leq R)$
Step 2. For $i = 1$ to R do the following:
Call $Func(1, i)$
Step 3. Output LB_R

$Func(x, r)$
Step 4. If $x = NF_r + 1$ do the following:
If $LB_r > \sum_{p=1}^{NF_r} \mathcal{D}_p$, $LB_r \leftarrow \sum_{p=1}^{NF_r} \mathcal{D}_p$.
Step 5. If $x \neq NF_r + 1$. For $j = 0$ to m do the following:
Set $\mathcal{D}_x = j$ and check whether all properties
for the target structure are satisfied or not.
If the check is OK do the following:
Step 5.1. If $x \notin \{NF_k | 1 \leq k \leq r - 1\}$
Call $Func(x + 1, r)$.
Step 5.2. If $x \in \{NF_k | 1 \leq k \leq r - 1\}$
Let z be an integer satisfying $x = NF_z$.
If $\sum_{p=1}^{NF_z} \mathcal{D}_p + LB_{r-z} \leq LB_r$,
call $Func(x + 1, r)$.

At Step 5.2., if the total of a) the sum of determined active S-boxes in the first z F-functions, and b) the known lower bound for the rest of rounds, already exceeds c) temporary lower bounds LB_y of the current target number y, further searches are aborted because this situation never gives a better lower bound. The branch cutting with an early-abort approach can significantly reduce the search effort. Our implementation result shows that a search for 100-round Type-I Feistel structures when $m = 4$, $d = 4$ can be obtained within a few tens of seconds by the improved algorithm. This improvement enables us to evaluate many types of structures.

5.3 Experimental Results

By using the improved algorithm, we first compared the lower bounds of Type-I, Type-II and Nyberg's generalized Feistel structure for both cases using and not using the DSM technique. The chosen parameters for each structure are $m = 4$, $d = 4$ and ${}^*B_1^D = {}^*B_2^D = {}^*B_2^L = 5$. Tables 3 and 4 show the results of estimation for 40-round Type-I structure and 20-round Type-II and Nyberg's structures, therefore each structure contains 40 F-functions.

5.4 Discussion and Comparison

From the above, we confirmed that the all lower bounds obtained by the search algorithm are larger than that obtained by the rough estimation method described in the previous section. For these parameters, the rough estimation methods implies 10, 20 and 30 active S-boxes for 12, 24 and

Table 3 Estimation results.

	Type-I				Type-I		
r	none	D	L	r	none	D	L
1	0	0	0	21	19	21	24
2	0	0	0	22	19	22	25
3	0	0	0	23	20	25	28
4	1	1	1	24	24	26	29
5	1	1	1	25	24	27	31
6	1	1	1	26	25	28	32
7	2	2	5	27	25	31	34
8	6	6	6	28	26	32	35
9	6	6	6	29	27	34	36
10	7	7	10	30	31	36	38
11	7	8	11	31	32	36	38
12	8	11	13	32	34	37	38
13	9	12	15	33	35	39	41
14	13	15	16	34	35	40	42
15	14	16	17	35	36	41	43
16	16	16	18	36	36	41	45
17	17	17	20	37	37	42	47
18	17	20	20	38	37	45	49
19	18	20	20	39	38	46	50
20	18	21	23	40	42	47	52

none : Num. of diff. and linear active S-boxes w/o DSM
D : Num. of diff. active S-boxes with DSM
L: Num. of linear active S-boxes with DSM

Table 4 Estimation results.

	Type-II				Nyberg's		
r	none	D	L	r	none	D	L
1	0	0	0	1	0	0	0
2	1	1	1	2	0	0	0
3	2	2	5	3	1	1	1
4	6	6	6	4	2	2	5
5	8	8	10	5	5	6	6
6	12	12	15	6	6	10	10
7	12	14	16	7	7	10	10
8	13	18	18	8	8	11	11
9	14	20	20	9	9	12	15
10	18	22	23	10	10	12	15
11	20	24	26	11	11	16	16
12	24	28	30	12	12	20	20
13	24	30	32	13	13	20	20
14	25	34	34	14	14	21	21
15	26	36	36	15	15	22	25
16	30	38	38	16	16	22	25
17	32	40	40	17	17	26	26
18	36	44	44	18	18	30	30
19	36	46	46	19	19	30	30
20	37	50	50	20	20	31	31

36 rounds of Type-I structure, and also for 6, 12 and 18 rounds of Type-II structure. In all cases, the search algorithm outputs tighter lower bounds for the chosen parameters. This means that the method for roughly estimating lower bounds does not always give tight bounds. Therefore we expect improved results of the method which guarantees tighter bounds in further research. Now we leave this problem open.

Also we see that the obtained results show the effect of DSM in all three structures. Although we provide estimated data only for the limited case in the table, we confirmed similar results for the cases using other parameter sets.

Furthermore, it is shown that the guaranteed numbers per F-function of active S-boxes of Nyberg's Feistel structure are explicitly smaller than those of Type-I and Type-II structures, and it is also shown that Type-I and Type-II have the same level of immunity against differential attack and linear attack which is already implied by proven lower bounds in Sect. 4. The slower diffusion effect of Nyberg's structure is due to the fact that there is a 2-round iterative differential (or linear) characteristic which contains only one active s-boxes in a round in case $d = 4$. Similar iterative characteristics are also found for other d. This implies that that Nyberg's generalized Feistel structure does not offer better immunity against differential and linear attack than Type-I and Type-II structure when SP-type F-functions are used for them.

6. Conclusion

We have derived lower bounds of Type-I and Type-II generalized Feistel structures which use DSM technique. The results showed that both structures have the same level of numbers of estimated active S-boxes per an F-function, which implies that Type-II structure is expected to hold practical advantage over Type-I with regard to the processing speed. Moreover, we showed an improved search algorithm to find lower bounds efficiently, and the experimental results revealed that DSM has explicit effect on all of these structures. We also showed that Nyberg structure doesn't guarantee as many active S-boxes as Type-I and Type-II structures when using SP-type F-functions.

Acknowledgements

We thank Kyoji Shibutani and anonymous reviewers of earlier versions of this paper for helpful comments.

References

[1] J. Daemen and V. Rijmen, The Design of Rijndael: AES — The Advanced Encryption Standard (Information Security and Cryptography), Springer, 2002.
[2] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-bit block cipher." Primitive submitted to AES, 1998. Available at http://www.schneier.com/
[3] R. Anderson, E. Biham, and L.R. Knudsen, "Serpent: A proposal for the advanced encryption standard." Primitive submitted to AES, 1998. Available at http://www.cs.technion.ac.il/~biham/Reports/Serpent/
[4] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Camellia: A 128-bit block cipher suitable for multiple platforms," 2000. Available at http://info.isl.ntt.co.jp/crypt/camellia/dl/support.pdf
[5] P.S.L.M. Barreto and V. Rijmen, "The Whirlpool hashing function." Primitive submitted to NESSIE, Sept. 2000. Available at http://www.cryptonessie.org/
[6] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
[7] M. Matsui, "Linear cryptanalysis of the data encryption standard," Proc. Eurocrypt'93, ed. T. Helleseth, LNCS, no.765, pp.386–397, 1994.

[8] M. Kanda, "Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function," Proc. Selected Areas in Cryptography — SAC'00, ed. D.R. Stinson and S.E. Tavares, LNCS, no.2012, pp.324–338, 2001.
[9] T. Shirai, S. Kanamaru, and G. Abe, "Improved upper bounds of differential and linear characteristic probability for Camellia," Proc. Fast Software Encryption — FSE'02, ed. J. Daemen and V. Rijmen, LNCS, no.2365, pp.128–142, 2002.
[10] Data Encryption Standard, "Federal information processing standard (FIPS)," National Bureau of Standards, U.S. Department of Commerce, Washington D.C., Jan. 1977.
[11] M. Matsui, "Differential path search of the block cipher E2," ISEC Technical Report — ISEC99-19, 1999.
[12] Y. Zheng, T. Matsumoto, and H. Imai, "On the construction of block ciphers provably secure and not relying on any unproved hypotheses," Proc. Crypto'89, ed. G. Brassard, LNCS, no.435, pp.461–480, 1989.
[13] K. Nyberg, "Generalized Feistel network," Proc. Asiacrypt'96, ed. K. Kim and T. Matsumoto, LNCS, no.1163, pp.91–104, 1996.
[14] R.L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, "The RC6 block cipher." Primitive submitted to AES, 1998. Available at http://www.rsasecurity.com/
[15] S. Moriai and S. Vaudenay, "On the pseudorandomness of top-level schemes of block ciphers," Proc. Asiacrypt'00, ed. T. Okamoto, LNCS, no.1976, pp.289–302, 2000.
[16] L.R. Knudsen and D. Wagner, "Integral cryptanalysis," Proc. Fast Software Encryption — FSE'02, ed. J. Daemen and V. Rijmen, LNCS, no.2365, pp.112–127, 2002.
[17] J. Kim, S. Hong, J. Sung, C. Lee, and S. Lee, "Impossible differential cryptanalysis for block cipher structure," Proc. Indocrypt 2003, ed. T. Johansson and S. Maitra, LNCS, no.2904, pp.82–96, 2003.
[18] W. Wu, W. Zhang, and D. Lin, "Security on generalized Feistel scheme with SP round function," Int. J. Network Security, vol.3, no.3, pp.215–224, 2006.
[19] T. Shirai and K. Shibutani, "Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices," Proc. Fast Software Encryption — FSE'04, ed. B. Roy and W. Meier, LNCS, no.3017, pp.260–278, 2004.
[20] T. Shirai and B. Preneel, "On Feistel ciphers using optimal diffusion mappings across multiple rounds," Proc. Asiacrypt'04, ed. P.J. Lee, LNCS, no.3329, pp.1–15, 2004.
[21] T. Shirai and K. Shibutani, "On Feistel structures using a diffusion switching mechanism," Proc. Fast Software Encryption — FSE'06, ed. M. Robshaw, LNCS, no.4047, pp.41–56, 2006.
[22] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA," Proc. Fast Software Encryption — FSE'07, ed. A. Biryukov, LNCS, no.4593, pp.181–195, 2007.
[23] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

Taizo Shirai was born in 1973. He received his B.Eng. and M.Eng. degrees from Tokyo Institute of Technology, Tokyo Japan, in 1996 and 1998, respectively. He is a researcher in Sony Corporation. He is presently engaged in research on information security. In 2003–2004 he was a visiting researcher at Katholieke Universiteit Leuven, Belgium. He is a member of the International Association for Cryptologic Research (IACR).

Kiyomichi Araki was born in 1949. He received the B.S. degree in Electrical Engineering from Saitama University, in 1971, and the M.S. and Ph.D. degrees in Physical Electronic from Tokyo Institute of Technology in 1973 and 1978, respectively. In 1973–1975, and 1978–1985, he was a research Associate at Tokyo Institute of Technology, and in 1985–1995 he was an Associate Professor at Saitama University. In 1979–1980 and 1993–1994 he was a visiting research scholar at University of Texas, Austin and University of Illinois, Urbana, respectively. Since 1995 he has been a Professor at Tokyo Institute of Technology. Dr. Araki is a member of IEEE, IEE of Japan and Information Society of Japan. His research interests are in information security, coding theory, communication theory, ferrite devices, RF circuit theory, electromagnetic theory, software defined radio, array signal processing, UWB technologies, wireless channel modeling and so on.