On Feistel Structures Using a Diffusion Switching Mechanism

Taizo Shirai and Kyoji Shibutani

Sony Corporation, Tokyo, Japan
{Taizo.Shirai, Kyoji.Shibutani}@jp.sony.com

Abstract. We study a recently proposed design approach of Feistel structure which employs diffusion matrices in a switching way. At ASIACRYPT 2004, Shirai and Preneel have proved that large numbers of S-boxes are guaranteed to be active if a diffusion matrix used in a round function is selected among multiple matrices. However the optimality of matrices required by the proofs sometimes pose restriction to find matrices suitable for actual blockciphers. In this paper, we extend their theory by replacing the condition of optimal mappings with general-type mappings, consequently the restriction is eliminated. Moreover, by combining known lower bounds for usual Feistel structure, we establish a method to estimate the guaranteed number of active S-boxes for arbitrary round numbers. We also demonstrate how the generalization enables us to mount wide variety of diffusion mappings by showing concrete examples.

Keywords: blockcipher, Feistel structure, optimal diffusion mappings.

1 Introduction

A Feistel structure is one of the most widely used and best studied structures for the design of blockciphers. It was proposed by H. Feistel in the early 1970s; subsequently the structure was adopted in the well-known blockcipher DES [6,7]. During the 30-year of modern blockcipher research history, extensive studies have been made on Feistel structure [10, 13, 16]. Currently, many well-known blockciphers employ the design of Feistel structures [1, 12, 15, 17].

On the other hand, an optimal diffusion which is a linear function with the maximum branch number is widely regarded in the recent blockcipher research; the concept is used in the design of AES/Rijndael and many other cryptographic primitives [2, 17, 14, 5]. However the effect of an optimal diffusion especially in Feistel structure is still needed to be studied.

In 2004, Shirai and Shibutani proposed a novel design concept of Feistel structure which employs plural optimal diffusion matrices in a switching manner. In their design approach, a diffusion matrix in the round function is switched among multiple matrices in a predefined order [21]. We call the matrix switching technique *Diffusion Switching Mechanism* (*DSM* for short) in this paper. Then, Shirai and Preneel has first shown the theoretical explanation of the effects of the

M.J.B. Robshaw (Ed.): FSE 2006, LNCS 4047, pp. 41–56, 2006.

DSM [19]. They proved that the immunity against both differential and linear cryptanalysis would be strengthened due to the fact that difference and linear mask cancellation in characteristics caused by a small number of active S-boxes will never occur.

The theory of the *DSM* opened a new line of research on the Feistel structure. However the optimality condition for matrices in their result sometimes pose restriction to find various matrices suitable for actual blockciphers. For example, our experimental result showed that there are no 8 × 8 matrices over $GF(2^8)$ satisfying both the optimality and certain practically favorable conditions.

In this paper, we generalize the *DSM* theory by eliminating the conditions of diffusion mappings. This generalization enables us to estimate the guaranteed number of active S-boxes for any types of diffusion mappings if we get knowledge of branch numbers of the mappings. Let a minimum differential branch number among all diffusion matrices used in the Feistel structure be B_1^D, and let a smallest differential and a linear branch number of diffusion matrices composed of two alternate (i.e. i-th and $i+2$-th) rounds be B_2^D, B_2^L, respectively, and three alternate $(i, i+2, i+4$-th) rounds differential branch number be B_3^D. Then, we prove novel extended result on the numbers of active S-boxes such that $R(B_1^D + B_2^D)$ differential active S-boxes for $6R$-round, $R(2B_1^D + B_3^D)$ for $9R$-round and RB_2^L linear active S-boxes for $3R$-round are theoretically guaranteed.

In addition, we show how to estimate the lower bound of number of active S-boxes for arbitrary number of rounds. Kanda has already shown the results on lower bound of the number of active S-boxes for single matrix based ordinary Feistel structure [9]. By combining our results and Kanda's results, lower bounds for any number of rounds can be calculated in a simple manner. Consequently, we can make use of the proved lower bounds for designing Feistel ciphers which hold desirable expected immunity against differential attack and linear attack [4]. We also confirm effects of the generalization by showing concrete example 8 × 8 matrices for a 128-bit block Feistel structure.

This paper is organized as follows: in Sect. 2, we introduce some definitions used in this paper. Previous works including *ODM-MR design* approach are shown in Sect. 3. We prove in Sect. 4 the extended theorems regarding *Diffusion Switching Mechanism* (*DSM* for short) as our main contribution. In Sect. 5, we discuss the new design approach by presenting some examples and numerical values. Finally Sect. 6 concludes the paper.

2 Preliminaries

In this paper, we treat a typical type of Feistel structure, which is called a balanced Feistel. It is defined as follows [16].

Definition 1. *(Balanced Feistel structure)*
Let b be a block size, r be a number of rounds, and k be a size of round key. Let $k_i \in \{0,1\}^k$ $(1 \leq i \leq r)$ be round keys provided by a certain key scheduling algorithm and $x_i \in \{0,1\}^{b/2}$ be intermediate data, and let $F_i : \{0,1\}^{b/2} \times$

$\{0,1\}^k \rightarrow \{0,1\}^{b/2}$ be an F-function at the i-th round. The algorithm of a balanced Feistel structure is defined as : (1) Input $x_0, x_1 \in \{0,1\}^{b/2}$, (2) Calculate $x_{i+1} = F_i(x_i, k_i) \oplus x_{i-1}$ $(1 \leq i \leq r)$, (3) Output $x_r, x_{r+1} \in \{0,1\}^{b/2}$.

Then we define SP-type F-functions which are special constructions of a F-function [18, 9].

Definition 2. *(SP-type F-functions)*
Let a length of a round key $k = b/2$. Let m be the number of S-boxes in a round, and n be the size of the S-boxes, with $mn = b/2$. Let $s_{i,j} : \{0,1\}^n \rightarrow \{0,1\}^n$ be the j-th S-box in the i-th round, and let $S_i : \{0,1\}^{b/2} \rightarrow \{0,1\}^{b/2}$ be the function generated by concatenating m S-boxes in parallel in the i-th round. Let $P_i : \{0,1\}^{b/2} \rightarrow \{0,1\}^{b/2}$ be the linear Boolean function. Then SP-type F-functions are defined as $F_i(x_i, k_i) = P_i(S_i(x_i \oplus k_i))$.

Note that we denote the intermediate variables $z_i = S_i(x_i \oplus k_i)$ in this paper.

Definition 3. *((m,n,r)-SPFS)*
An (m,n,r)-SPFS is defined as an r-round Feistel structure with SP-type round function using m n-bit S-boxes, and for which all $s_{i,j}$, P_i are bijective. An $mn \times mn$ matrix M_i $(1 \leq i \leq r)$ over $GF(2)$ denotes a matrix representation of a linear Boolean function P_i where $P_i(x) = M_i x$.

Remark 1. Because of the bijectivity of S-boxes and linear function P in (m,n,r)-SPFS, all F-functions are bijective.

We also give definitions of bundle weight and branch number [5].

Definition 4. *(bundle weight)*
Let $x \in \{0,1\}^{pn}$ represented as $x = [x_0 x_1 \ldots x_{p-1}]$ where $x_i \in \{0,1\}^n$, then the bundle weight $w_n(x)$ is defined as

$$w_n(x) = \sharp\{x_i | x_i \neq 0\} \ .$$

Definition 5. *(Branch Number)*
Let $P : \{0,1\}^{pn} \rightarrow \{0,1\}^{qn}$. The branch number of P is defined as

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

Remark 2. The maximum branch number is $\mathcal{B}r_n(P) = q + 1$. If a linear function has a maximum branch number, it is called an **optimal diffusion mapping** [2]. It is known that an optimal diffusion mapping can be obtained from maximum distance separable (MDS) codes [5].

3 Previous Work

The precise estimation of the lower bound of the number of active S-boxes of blockciphers has been known as one of the practical means to evaluate strength of ciphers, because the lower bound can be used to estimate weight distributions of differential and linear characteristics [11,3,1,18,9,5]. It is shown that the weight distribution is connected with the bound of the expected differential probability or the linear hull probability by Daemen and Rijmen [4].

Recently, Shirai and Preneel proved the following corollary which can be used to estimate the lower number of active S-boxes of a specially designed Feistel structure [21,19].

Definition 6. *Let p be a positive integer, and A, B be $p \times p$ square matrices. Then $[A|B]$ denotes a $p \times 2p$ matrix obtained by concatenating A and B. Similarly, the three matrices case is defined for $[A|B|C]$.*

Corollary 1. *Let E be an (m,n,r)-SPFS blockcipher where $r \geq 6$. If $[M_i|M_{i+2}|M_{i+4}]$ and $[{}^tM_j^{-1}|{}^tM_{j+2}^{-1}]$ are optimal diffusion mappings for any i, j $(1 \leq i \leq r-4, 1 \leq j \leq r-2)$, respectively, any $3R$ consecutive rounds $(R \geq 2)$ in E guarantee at least $R(m+1)$ differential and linear active S-boxes.*

The design approach is called *ODM-MR* (Optimal Diffusion Mappings across Multiple Rounds) design approach. To apply the corollary to practical Feistel structures, we need to use at least three different matrices [19]. For example, let A_0, A_1, A_2 be the matrices which satisfy the following conditions.

1. Choose $nm \times nm$ matrices A_0, A_1, A_2 over $GF(2)$ satisfying the following optimal diffusion conditions:
   (a) $\mathcal{B}r_n([A_0|A_1|A_2]) = m+1$,
   (b) $\mathcal{B}r_n([{}^tA_0^{-1}|{}^tA_1^{-1}]) = \mathcal{B}r_n([{}^tA_1^{-1}|{}^tA_2^{-1}]) = \mathcal{B}r_n([{}^tA_2^{-1}|{}^tA_0^{-1}]) = m+1$.
2. Set these three matrices as $M_{2i+1} = M_{2r-2i} = A_{\ i \ mod \ 3}$, for $0 \leq i < r$ in an $2r$-round Feistel structure $(m, n, 2r)$-SPFS (Fig.1).

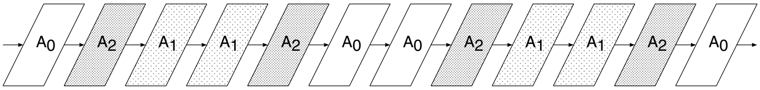

Fig. 1. Example Allocation of Matrices A_0, A_1, A_2

The corollary states that the $(m, n, 2r)$-SPFS with the above settings guarantees $2(m+1)$, $3(m+1)$ and $4(m+1)$ differential and linear active S-boxes in 6, 9 and 12 consecutive rounds, respectively. Fig. 2 illustrates the statement.

In this way, using multiple diffusion matrices in a switching way for round functions makes Feistel structure stronger against differential attack and linear attack. In this paper, we call the new design concept a *Diffusion Switching Mechanism* (DSM) in general. From now on, we will extend the DSM to treat not only optimal diffusion matrices but also any general type matrices.

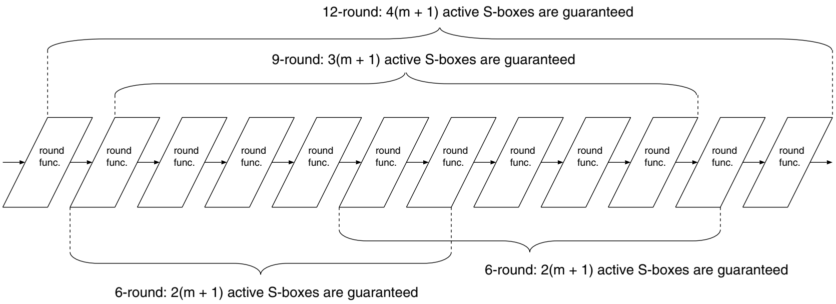
12-round: 4(m + 1) active S-boxes are guaranteed
9-round: 3(m + 1) active S-boxes are guaranteed
round func.
6-round: 2(m + 1) active S-boxes are guaranteed
6-round: 2(m + 1) active S-boxes are guaranteed

Fig. 2. Guaranteed Active S-boxes by *ODM-MR design*

4 DSM for General Matrices

In this section, we show the extended theory of the DSM theoretically[1]. The following two subsections are devoted to proving three theorems. To ease the proofs, we first introduce an additional definition.

Definition 7. *Consider differential characteristics or linear characteristics. Let D_i and L_i denote the number of differential and linear active S-boxes in the i-th round, respectively. These values are determined by the differences $\Delta x_i, \Delta z_i$ or by the linear masks $\Gamma x_i, \Gamma z_i$. Since all S-boxes are bijective, we have the following relations,*

$$D_i = w_n(\Delta x_i) = w_n(\Delta z_i) \ , \qquad L_i = w_n(\Gamma x_i) = w_n(\Gamma z_i) \ ,$$

where $w_n(\cdot)$ is the bundle weight as defined in Definition 4.

Remark 3. If we have a nonzero input difference for an (m, n, r)-SPFS, we obtain the following conditions:

$$\begin{array}{ll} (d0) & D_i = 0 \Rightarrow D_{i-2} \neq 0, D_{i-1} \neq 0, D_{i+1} \neq 0, D_{i+2} \neq 0 \ , \\ (d1) & D_i = 0 \Rightarrow D_{i-1} = D_{i+1} \ . \end{array}$$

Similarly, if a nonzero input mask is given, we have

$$\begin{array}{ll} (l0) & L_i = 0 \Rightarrow L_{i-2} \neq 0, L_{i-1} \neq 0, L_{i+1} \neq 0, L_{i+2} \neq 0 \ , \\ (l1) & L_i = 0 \Rightarrow L_{i-1} = L_{i+1} \ . \end{array}$$

4.1 Proofs for the Lower Bound of Differential Active S-Boxes

In this section we prove Theorem 1 and Theorem 2; the proof is based on three lemmata. Firstly we define a concept of minimum branch numbers for three types of matrices.

[1] The composition of the extended version of proofs almost follows that of proofs for *ODM-MR* [19].

Definition 8. *For an (m, n, r)-SPFS, minimum branch numbers B_1^D, B_2^D and B_3^D are defined as follows.*

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

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

$$B_3^D = \min_{1 \le i \le r-4} (\mathcal{B}r_n([M_i|M_{i+2}|M_{i+4}])) \ .$$

Obviously, the following inequality holds.

$$B_1^D \ge B_2^D \ge B_3^D \ . \tag{1}$$

Note that these values can be derived from any given set of diffusion mappings M_i $(1 \le i \le r)$. Introducing these values into the proofs means that the constraint of optimal diffusion mappings will disappear. This is an essence of our generalization.

Firstly, Lemma 1 shows relations between D_i of (m, n, r)-SPFS and B_1^D.

Lemma 1. *Let E be an (m, n, r)-SPFS blockcipher, then E has the following condition $(d2)$.*

$$(d2) \quad D_{i+1} \ne 0 \Rightarrow D_i + D_{i+1} + D_{i+2} \ge B_1^D \ .$$

Proof. From the relation between the differences Δz_{i+1},Δx_i and Δx_{i+2} in a 3 consecutive rounds, we obtain the following equation.

$$M_{i+1} \Delta z_{i+1} = \Delta x_i \oplus \Delta x_{i+2} \ .$$

Since M_i has a branch number at least B_1^D we have

$$w_n(\Delta z_{i+1}) \ne 0 \Rightarrow w_n(\Delta z_{i+1}) + w_n(\Delta x_i \oplus \Delta x_{i+2}) \ge B_1^D \ . \tag{2}$$

Eq. (2) and the inequality $w_n(\Delta x_i) + w_n(\Delta x_{i+2}) \ge w_n(\Delta x_i \oplus \Delta x_{i+2})$ yield $(d2)$. □

Remark 4. By combining Remark 3 and $(d2)$, we obtain additional underlying conditions $(d3)$ and $(d4)$.

$$(d3) \quad D_i = 0 \Rightarrow D_{i+1} + D_{i+2} \ge B_1^D \ ,$$
$$(d4) \quad D_{i+2} = 0 \Rightarrow D_i + D_{i+1} \ge B_1^D \ .$$

Eq. $(d3)$ and $(d4)$ mean that if a k-th round has no active S-boxes, any 2 consecutive rounds next to the k-th round always contain more than B_1^D active S-boxes.

Next, we show the property of (m, n, r)-SPFS for two matrices case.

Lemma 2. *Let E be an (m, n, r)-SPFS blockcipher, E has the following conditions $(d5), (d6)$.*

$$(d5) \quad D_{i+4} = 0 \Rightarrow D_i + D_{i+1} + D_{i+3} \ge B_2^D \ ,$$
$$(d6) \quad D_i = 0 \Rightarrow D_{i+1} + D_{i+3} + D_{i+4} \ge B_2^D \ .$$

Proof. From the relation between 5-round differences,

$$M_{i+1}\Delta z_{i+1} \oplus M_{i+3}\Delta z_{i+3} = \Delta x_i \oplus \Delta x_{i+4} \ .$$

Then,

$$[M_{i+1}|M_{i+3}] \begin{pmatrix} \Delta z_{i+1} \\ \Delta z_{i+3} \end{pmatrix} = \Delta x_i \oplus \Delta x_{i+4} \ .$$

Since $[M_{i+1}|M_{i+3}]$ has a branch number at least B_2^D, and from Remark 3, we see that $w_n(\Delta z_{i+1}) = 0$ and $w_n(\Delta z_{i+3}) = 0$ will never occur simultaneously, we obtain

$$w_n(\Delta z_{i+1}) + w_n(\Delta z_{i+3}) + w_n(\Delta x_i \oplus \Delta x_{i+4}) \geq B_2^D \ .$$

Assuming the cases $\Delta x_i = 0$ or $\Delta x_{i+4} = 0$, we directly obtain $(d5)$ and $(d6)$. □

By using the previously obtained conditions $(d0) - (d6)$, we show the following theorem for differential active S-boxes.

Theorem 1. *Let E be an (m, n, r)-SPFS blockcipher, any 6 consecutive rounds in E guarantee at least $B_1^D + B_2^D$ differential active S-boxes.*

Proof. Consider the total number of active S-boxes in 6 consecutive rounds from the i-th round,

$$\sum_{k=i}^{i+5} D_k = D_i + D_{i+1} + D_{i+2} + D_{i+3} + D_{i+4} + D_{i+5} \ .$$

If $D_{i+1} \neq 0$ and $D_{i+4} \neq 0$, the condition $(d2)$ guarantees that $D_i + D_{i+1} + D_{i+2} \geq B_1^D$ and $D_{i+3} + D_{i+4} + D_{i+5} \geq B_1^D$. Therefore we obtain $\sum_{k=i}^{i+5} D_k \geq 2B_1^D$.
If $D_{i+1} = 0$,

$$\sum_{k=i}^{i+5} D_k = D_i + D_{i+2} + D_{i+3} + D_{i+4} + D_{i+5} \ .$$

From $(d1)$,

$$\begin{aligned}\sum_{k=i}^{i+5} D_k &= 2 \cdot D_{i+2} + D_{i+3} + D_{i+4} + D_{i+5} \\ &= (D_{i+2} + D_{i+3}) + (D_{i+2} + D_{i+4} + D_{i+5}) \ .\end{aligned}$$

From $(d3)$ and $(d6)$,

$$\sum_{k=i}^{i+5} D_k \geq B_1^D + B_2^D \ .$$

The case of $D_{i+4} = 0$ is proved similarly from $(d1)$, $(d4)$ and $(d5)$. Combining with (1), we have shown that any 6 consecutive rounds in E guarantee at least $B_1^D + B_2^D$ differential active S-boxes. □

Immediately, we obtain the following corollary.

Corollary 2. *Let E be an (m, n, r)-SPFS blockcipher. Any $6R$ consecutive rounds in E guarantee at least $R(B_1^D + B_2^D)$ differential active S-boxes.*

The result is compatible with *ODM-MR* by substituting $m+1$ for B_1^D and B_2^D.

Next, we show the property of (m, n, r)-SPFS for three matrices case.

Lemma 3. *Let E be an (m, n, r)-SPFS blockcipher. E satisfies the following condition $(d7)$.*

$$(d7) \quad D_i = D_{i+6} = 0 \Rightarrow D_{i+1} + D_{i+3} + D_{i+5} \geq B_3^D \ .$$

Proof. First, from the difference relation in 7 consecutive rounds, we obtain

$$M_{i+1}\Delta z_{i+1} \oplus M_{i+3}\Delta z_{i+3} \oplus M_{i+5}\Delta z_{i+5} = \Delta x_i \oplus \Delta x_{i+6} \ .$$

Then,

$$[M_{i+1}|M_{i+3}|M_{i+5}] \begin{pmatrix} \Delta z_{i+1} \\ \Delta z_{i+3} \\ \Delta z_{i+5} \end{pmatrix} = \Delta x_i \oplus \Delta x_{i+6} \ .$$

Since $[M_{i+1}|M_{i+3}|M_{i+5}]$ has a branch number at least B_3^D, and from Remark 3, $w_n(\Delta z_{i+1})$, $w_n(\Delta z_{i+3})$, and $w_n(\Delta z_{i+5})$ cannot be simultaneously 0, we get that

$$w_n(\Delta z_{i+1}) + w_n(\Delta z_{i+3}) + w_n(\Delta z_{i+5}) + w_n(\Delta x_i \oplus \Delta x_{i+6}) \geq B_3^D \ .$$

By assuming $\Delta x_i = 0$ and $\Delta x_{i+6} = 0$, we derive the condition $(d7)$. □

From the additional condition $(d7)$, we derive the following theorem.

Theorem 2. *Let E be an (m, n, r)-SPFS blockcipher. Any 9 consecutive rounds in E guarantee at least $2B_1^D + B_3^D$ differential active S-boxes.*

Proof. Consider the total number of active S-boxes in 9 consecutive rounds,

$$\sum_{k=i}^{i+8} D_k = D_i + D_{i+1} + D_{i+2} + D_{i+3} + D_{i+4} + D_{i+5} + D_{i+6} + D_{i+7} + D_{i+8} \ .$$

If $D_{i+1} \neq 0$ then $D_i + D_{i+1} + D_{i+2} \geq B_1^D$ from (d2), and Lemma 1 guarantees that the sum of the remaining 6 consecutive rounds $\sum_{k=i+3}^{i+8} D_k \geq B_1^D + B_2^D$. Consequently $\sum_{k=i}^{i+8} D_k \geq 2B_1^D + B_2^D$. Similarly, if $D_{i+7} \neq 0$, at least $2B_1^D + B_2^D$ active S-boxes are guaranteed.

If $D_{i+1} = D_{i+7} = 0$, we obtain

$$\sum_{k=i}^{i+8} D_k = D_i + D_{i+2} + D_{i+3} + D_{i+4} + D_{i+5} + D_{i+6} + D_{i+8} \ .$$

From $(d1)$,

$$\begin{aligned} \sum_{k=i}^{i+8} D_k &= 2 \cdot D_{i+2} + D_{i+3} + D_{i+4} + D_{i+5} + 2 \cdot D_{i+6} \\ &= (D_{i+2} + D_{i+3}) + (D_{i+2} + D_{i+4} + D_{i+6}) + (D_{i+5} + D_{i+6}) \ . \end{aligned}$$

From $(d3)$, $(d7)$ and $(d4)$,

$$\sum_{k=i}^{i+8} D_k \geq B_1^D + B_3^D + B_1^D = 2B_1^D + B_3^D \ .$$

Combining with (1), we have shown that any 9 consecutive rounds in E guarantee at least $2B_1^D + B_3^D$ differential active S-boxes. □

Immediately, we obtain the following corollary.

Corollary 3. *Let E be an (m, n, r)-SPFS blockcipher. Any $9R$ consecutive rounds in E guarantee at least $R(2B_1^D + B_3^D)$ differential active S-boxes.*

The result is compatible with *ODM-MR* by substituting $m + 1$ for B_1^D and B_3^D.

4.2 Proofs for the Lower Bound of Linear Active S-Boxes

In this subsection, we will show the proof of the guaranteed number of linear active S-boxes of (m, n, r)-SPFS.

Definition 9. *For an (m, n, r)-SPFS, minimum branch number B_2^L is defined as follows.*

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

Theorem 3. *Let E be an (m, n, r)-SPFS blockcipher. Any 3 consecutive rounds in E has at least B_2^L linear active S-boxes.*

Proof. From the 3-round linear mask relation,

$$\Gamma x_{i+1} = {}^tM_i^{-1} \Gamma z_i \oplus {}^tM_{i+2}^{-1} \Gamma z_{i+2} \ .$$

Then,

$$\Gamma x_{i+1} = [{}^tM_i^{-1} | {}^tM_{i+2}^{-1}] \begin{pmatrix} \Gamma z_i \\ \Gamma z_{i+2} \end{pmatrix} \ .$$

Since $[{}^tM_i^{-1} | {}^tM_{i+2}^{-1}]$ has a branch number at least B_2^L, and from Remark 3, $w_n(\Gamma z_i)$ and $w_n(\Gamma z_{i+2})$ cannot be simultaneously 0, we obtain

$$w_n(\Gamma z_i) + w_n(\Gamma x_{i+1}) + w_n(\Gamma z_{i+2}) \geq B_2^L \ .$$

By using the notion of L_i, this implies,

$$(l1) \quad L_i + L_{i+1} + L_{i+2} \geq B_2^L \ .$$

□

As a result, we obtain the following corollary.

Corollary 4. *Let E be an (m, n, r)-SPFS blockcipher. Any $3R$ consecutive rounds in E guarantee at least RB_2^L linear active S-boxes.*

The result is compatible with *ODM-MR* by substituting $m + 1$ for B_2^L in the corollary 1.

5 Discussion

5.1 Comparison of the Results

The statement of the corollaries 2 and 3 are independently applicable. Therefore, it is possible that the both of these corollaries may produce different lowrbounds for the same round numbers.

For example, consider an $(m, n, 18R)$-SPFS, $3R(B_1^D + B_2^D)$ and $2R(2B_1^D + B_3^D)$ differential active S-boxes are lower bounded by the corollary 2 and 3, respectively. Letting two parameters of diffusion matrices $\alpha = B_1^D - B_2^D$ and $\beta = B_2^D - B_3^D$, we obtain the gap of these lower bounds as,

$$\begin{aligned} 3R(B_1^D + B_2^D) - 2R(2B_1^D + B_3^D) &= R(2(B_2^D - B_3^D) - (B_1^D - B_2^D)) \\ &= R(2\beta - \alpha) \end{aligned}$$

If $\alpha = 2\beta$, these lower bounds always coincide. If $\alpha \neq 2\beta$, different lower bounds are produced at the 18R-th rounds. In such a case, we had better choose a larger lower bound and use it to adjust lower bounds for the rounds after the 18-th rounds to get more precise estimation.

5.2 Interpolation for Skipped Rounds

The corollaries 2, 3 and 4 are not able to provide lower bounds for any number of rounds, because they are valid for only multiples of 3, 6, or 9 rounds. Besides these corollaries, we use known results for Feistel structure to interpolate guaranteed lower bounds of the rounds which are not indicated by these corollaries.

Firstly the following trivial conditions are described explicitly.

$$\text{(1-round cond.)} \quad D_i \geq 0, \quad L_i \geq 0 \ .$$

$$\text{(2-round cond.)} \quad D_i + D_{i+1} \geq 1 \ , \quad L_i + L_{i+1} \geq 1 \ .$$

Kanda has proved inequalities for 3 and 4-round for the single matrix based normal Feistel structure, which can be converted into our settings as follows [9].

$$\text{(3-round cond.)} \quad D_i + D_{i+1} + D_{i+2} \geq 2 \ .$$

$$\text{(4-round cond.)} \quad D_i + D_{i+1} + D_{i+2} + D_{i+3} \geq B_1^D \ .$$

Additionally, we use the following 5-round condition. The proof will be appeared in the appendix A.

$$\text{(5-round cond.)} \quad D_i + D_{i+1} + D_{i+2} + D_{i+3} + D_{i+4} \geq B_1^D + 1 \ .$$

We make use of these lower bounds for less than 5 consecutive rounds for differential active S-boxes and less than 2 consecutive rounds for linear active S-boxes to obtain the lower bounds for arbitrary round numbers.

5.3 Example Choice of Matrices

Here, we will demonstrate how to apply the generalized DSM theory to concrete Feistel structure to enhance the immunity against differential attack and linear attack by illustrating example matrices.

Let A_0, A_1 and A_2 be 8×8 matrices over $GF(2^8)$ with irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1 = 0$ as follows:

$$A_0 = \begin{pmatrix} 1&9&2&5&8&1&4&1 \\ 1&1&9&2&5&8&1&4 \\ 4&1&1&9&2&5&8&1 \\ 1&4&1&1&9&2&5&8 \\ 8&1&4&1&1&9&2&5 \\ 5&8&1&4&1&1&9&2 \\ 2&5&8&1&4&1&1&9 \\ 9&2&5&8&1&4&1&1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1&6&8&9&6&9&5&1 \\ 1&1&6&8&9&6&9&5 \\ 5&1&1&6&8&9&6&9 \\ 9&5&1&1&6&8&9&6 \\ 6&9&5&1&1&6&8&9 \\ 9&6&9&5&1&1&6&8 \\ 8&9&6&9&5&1&1&6 \\ 6&8&9&6&9&5&1&1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1&6&4&8&4&5&8&9 \\ 9&1&6&4&8&4&5&8 \\ 8&9&1&6&4&8&4&5 \\ 5&8&9&1&6&4&8&4 \\ 4&5&8&9&1&6&4&8 \\ 8&4&5&8&9&1&6&4 \\ 4&8&4&5&8&9&1&6 \\ 6&4&8&4&5&8&9&1 \end{pmatrix}.$$

Note that we chose the matrix A_0 from Whirlpool hashing function's diffusion matrix for reference [2] [8].

Let A'_0, A'_1 and A'_2 be 64×64 matrices over $GF(2)$ which are equivalent to A_0, A_1 and A_2, respectively. These matrices have the following properties [3].

1. $\mathcal{B}r_8(A'_0) = \mathcal{B}r_8(A'_1) = \mathcal{B}r_8(A'_2) = 9$,
2. $\mathcal{B}r_8([A'_0|A'_1]) = \mathcal{B}r_8([A'_1|A'_2]) = \mathcal{B}r_8([A'_2|A'_0]) = 8$,
3. $\mathcal{B}r_8([A'_0|A'_1|A'_2]) = 8$,
4. $\mathcal{B}r_8([{}^tA'^{-1}_0|{}^tA'^{-1}_1]) = \mathcal{B}r_8([{}^tA'^{-1}_1|{}^tA'^{-1}_2]) = \mathcal{B}r_8([{}^tA'^{-1}_2|{}^tA'^{-1}_0]) = 8$.

Property 1 indicates that each matrix is an optimal diffusion mapping itself since the branch number is column number plus 1, but the properties 2-4 indicate the combined matrices made from these matrices are not optimal. Our experiment shows that there are no set of matrices satisfying the optimality of property 2-4 within the following searching space.

- Irreducible polynomial is $x^8 + x^4 + x^3 + x^2 + 1 = 0$,
- Each element of matrices is in hex values `{1,2,3,..,e,f}` $\in GF(2^8)$. They can be represented as at most 4-bit value.

Note that the searching space applied in finding the Whirlpool's diffusion matrix by the designers is subset of our searching space, and the smallness of the matrix elements is considered to contribute efficient implementations [20, 2].

Since we could not prepare optimal matrices in this setting, now we can make use of the previously obtained generalized theorems for Feistel structures using the above non-optimal matrices.

[2] The matrix is transposed so as to adjust our form $y = Mx$ not $y = xM$.

[3] The notion $\mathcal{B}r_8$ is defined in section 2.

5.4 Feistel Structures Using 2 or 3 Matrices in DSM

We consider two types of Feistel structures which belong to $(8, 8, 2r)$-SPFS. One is using two matrices, the other is using three matrices. These both structures can be used for 128-bit blockciphers due to $m = n = 8$. In appendix B, we will show the cases for 64-bit block Feistel structure as well.

Let F128A be an $(8, 8, 2r)$-SPFS which employs matrices A_0 and A_1 as M_{2i+1} $= M_{2r-2i} = A_{\ i\ mod\ 2}$ for $0 \leq i < r$ (see Fig 3 when $r = 6$).

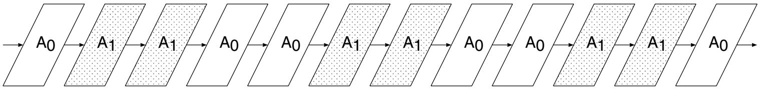

Fig. 3. Allocation of Matrices A_0, A_1 in F128A

Let F128B be an $(8, 8, 2r)$-SPFS which employs matrices A_0, A_1 and A_2 as $M_{2i+1} = M_{2r-2i} = A_{\ i\ mod\ 3}$ for $0 \leq i < r$ (see Fig 4 when $r = 6$).

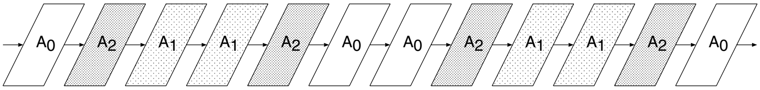

Fig. 4. Allocation of Matrices A_0, A_1, A_2 in F128B

In the above situation, we know that in F128A, $B_1^D = 9, B_2^D = 8, B_2^L = 8$, and the corollaries 2, 4 and conditions in Sect.5.2 are effective. On the other hand, in F128B, $B_1^D = 9, B_2^D = 8, B_3^D = 8, B_2^L = 8$, and the corollaries 2, 3, 4 and conditions in Sect.5.2 are effective.

The results of the guaranteed number of active S-boxes for F128A and F128B with other additional information are shown in the Table 1. Columns labeled by 'Dif.' and 'Lin.' contain lower bounds of differential and linear active S-boxes, respectively. Additionally, we show the lower bounds for the weights of the characteristics, which is simply calculated by multiplying the lower bound and a index number of maximum differential or linear probability of S-boxes [4]. The considered S-boxes here have the maximum differential probability 2^{-6} and 2^{-5}, maximal linear probability 2^{-6} and $2^{-4.39}$ for reference[4].

These weights of characteristics can be used to practically estimate the strength of the cipher against differential attack and linear attack [4]. In this case, the weight value should be larger than 128 with reasonable margin, for example 10-round F128A and 9-round F128B using 2^{-6} S-box and 12-round F128A, F128B using the second S-box seem to hold minimum security. The difference between F128A and F128B is only the value of lower bound for 9-round

[4] The value 2^{-6} is known best probability, 2^{-5} and $2^{-4.39}$ are experimentally obtained values that can be achieved by randomly chosen S-boxes in reasonable trials [4].

Table 1. Lower Bounds of Number of Active S-boxes and Weights of Characteristics

	F128A							F128B		
round	Dif.	DP_{max} 2^{-6}	DP_{max} 2^{-5}	Lin.	LP_{max} 2^{-6}	LP_{max} $2^{-4.39}$	speed (cycles/byte)	Dif.	Lin.	speed (cycles/byte)
1	**0**	0	0	**0**	0	0	-	**0**	**0**	-
2	**1**	6	5	**1**	6	4.39	-	**1**	**1**	-
3	**2**	12	10	**8**	48	35.12	-	**2**	**8**	-
4	**9**	54	45	**8**	48	35.12	-	**9**	**8**	-
5	**10**	60	50	**9**	54	39.51	-	**10**	**9**	-
6	**17**	102	85	**16**	96	70.24	-	**17**	**16**	-
7	**17**	102	85	**16**	96	70.24	-	**17**	**16**	-
8	**18**	108	90	**17**	102	74.63	-	**18**	**17**	-
9	**19**	114	95	**24**	144	105.36	-	**26**	**24**	-
10	**26**	156	130	**24**	144	105.36	11.38	**26**	**24**	11.65
11	**27**	162	135	**25**	150	109.75	-	**27**	**25**	-
12	**34**	204	170	**32**	192	140.48	13.60	**34**	**32**	14.11
13	**34**	204	170	**32**	192	140.48	-	**34**	**32**	-
14	**35**	210	175	**33**	198	144.87	15.75	**35**	**33**	16.37
15	**36**	216	180	**40**	240	175.6	-	**36**	**40**	-
16	**43**	258	215	**40**	240	175.6	17.93	**43**	**40**	18.70
17	**44**	264	220	**41**	246	179.99	-	**44**	**41**	-
18	**51**	306	255	**48**	288	210.72	19.88	**52**	**48**	20.64

and 18-round of differential active S-boxes. It implies that if 9-rounds immunity against differential attack is important, usage of 3 matrices should be taken into consideration.

Additionally, we mention a software implementation aspect. Software performance (in cycles per byte) of a moderately optimized C implementation of the F128A and F128B are measured on AMD Athlon64 4000+ (2.41GHz) with Windows XP Professional x64 Edition and Visual Studio .NET 2003. To use the lookup-table based implementation suitable for a 64-bit CPU, F128A requires a 32KB table (8 × 8-bit input × 64-bit output × 2 matrices) and F128B requires a 48KB table (3 matrices) [2]. Though they need large tables, we confirm that they achieve practically enough speed in this environment.

From the above observation, it is revealed that our novel results can be used to theoretically estimate the strength of Feistel structures using *DSM*.

6 Conclusion

We provide extended theory for the guaranteed number of active S-boxes of Feistel structure with DSM, which is realized by replacing the condition of optimal mappings with general mappings. As a result, we established a simple tool to evaluate any rounds of Feistel structures using DSM which employs arbitrary types of diffusion matrices. The effects of the novel result are confirmed by evaluating certain Feistel structures with concrete example matrices.

Acknowledgments. We thank Shiho Moriai for helpful discussions and suggestions. We also thank anonymous referees for their valuable comments.

References

1. 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." in *Proceedings of Selected Areas in Cryptography – SAC 2000* (D. R. Stinson and S. E. Tavares, eds.), no. 2012 in LNCS, pp. 41–54, Springer-Verlag, 2001.
2. P. S. L. M. Barreto and V. Rijmen, "The Whirlpool hashing function." Primitive submitted to NESSIE, Sept. 2000. Available at `http://www.cryptonessie.org/`.
3. E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems." *Journal of Cryptology*, vol. 4, pp. 3–72, 1991.
4. J. Daemen and V. Rijmen, "Statistics of correlation and differentials in block ciphers." in *IACR ePrint archive 2005/212*, 2005.
5. J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard (Information Security and Cryptography)*. Springer, 2002.
6. H. Feistel, "Cryptography and computer privacy." *Scientific American*, vol. 228, pp. 15–23, May 1973.
7. Data Encryption Standard, "Federal Information Processing Standard (FIPS)." National Bureau of Standards, U.S. Department of Commerce, Washington D.C., Jan. 1977.
8. International Organization for Standardization, "ISO/IEC 10118-3: Information Technology - Security Techniques - Hash-functions - Part 3: Dedicated hash-functions." 2003.
9. M. Kanda, "Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function." in *Proceedings of Selected Areas in Cryptography – SAC'00* (D. R. Stinson and S. E. Tavares, eds.), no. 2012 in LNCS, pp. 324–338, Springer-Verlag, 2001.
10. M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions." *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.
11. M. Matsui, "Linear cryptanalysis of the data encryption standard." in *Proceedings of Eurocrypt'93* (T. Helleseth, ed.), no. 765 in LNCS, pp. 386–397, Springer-Verlag, 1994.
12. M. Matsui, "New structure of block ciphers with provable security against differential and linear cryptanalysis." in *Proceedings of Fast Software Encryption – FSE'96* (D. Gollmann, ed.), no. 1039 in LNCS, pp. 205–218, Springer-Verlag, 1996.
13. K. Nyberg and L. R. Knudsen, "Provable security against a differential cryptanalysis." in *Proceedings of Crypto'92* (E. F. Brickell, ed.), no. 740 in LNCS, pp. 566–574, Springer-Verlag, 1993.
14. V. Rijmen, J. Daemen, B. Preneel, A. Bossalaers, and E. D. Win, "The cipher SHARK." in *Proceedings of Fast Software Encryption – FSE'96* (D. Gollmann, ed.), no. 1039 in LNCS, pp. 99–111, Springer-Verlag, 1996.
15. 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/`.
16. B. Schneier and J. Kelsey, "Unbalanced Feistel networks and block cipher design." in *Proceedings of Fast Software Encryption – FSE'96* (D. Gollmann, ed.), no. 1039 in LNCS, pp. 121–144, Springer-Verlag, 1996.

17. 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/`.
18. T. Shirai, S. Kanamaru, and G. Abe, "Improved upper bounds of differential and linear characteristic probability for Camellia." in *Proceedings of Fast Software Encryption – FSE'02* (J. Daemen and V. Rijmen, eds.), no. 2365 in LNCS, pp. 128–142, Springer-Verlag, 2002.
19. T. Shirai and B. Preneel, "On feistel ciphers using optimal diffusion mappings across multiple rounds." in *Proceedings of Asiacrypt'04* (P. J. Lee, ed.), no. 3329 in LNCS, pp. 1–15, Springer-Verlag, 2004.
20. T. Shirai and K. Shibutani, "On the diffusion matrix employed in the Whirlpool hashing function." NESSIE Public reports, 2003. Available at `http://www.cryptonessie.org/`.
21. T. Shirai and K. Shibutani, "Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices." in *Proceedings of Fast Software Encryption – FSE'04* (B. Roy and W. Meier, eds.), no. 3017 in LNCS, pp. 260–278, Springer-Verlag, 2004.

Appendix A

Here, we show the proof for the condition presented in the section 5.

By simply replacing the branch number symbol of the Kanda's Corollary 1 in [9] with our symbol B_1^D, we obtain

Corollary 5. *The minimum number of differential active S-boxes in any four consecutive rounds satisfies*

$$(i)\ D_i + D_{i+1} + D_{i+2} + D_{i+3} \geq B_1^D \textit{ if and only if } D_i = D_{i+3} = 0\ ,$$

$$(ii)\ D_i + D_{i+1} + D_{i+2} + D_{i+3} \geq B_1^D + 1 \textit{ in the other cases.}$$

Using the above corollary, we show the following lemma.

Lemma 4. *The minimum number of differential active S-boxes in any 5 consecutive rounds satisfies*

$$D_i + D_{i+1} + D_{i+2} + D_{i+3} + D_{i+4} \geq B_1^D + 1\ .$$

Proof. If $D_i \neq 0$ or $D_{i+3} \neq 0$, the inequality (ii) of the corollary 5 directly implies the above inequality. If $D_i = D_{i+3} = 0$, (i) implies $D_{i+1} + D_{i+2} \geq B_1^D$. By combining trivial condition $D_{i+3}+D_{i+4} \geq 1$, the desired condition is obtained immediately. □

Appendix B

Let A_0, A_1 and A_2 be 4×4 matrices over $GF(2^8)$ with irreducible polynomial $x^8 + x^4 + x^3 + x + 1 = 0$ as follows.

$$A_0 = \begin{pmatrix} 2&3&1&1 \\ 1&2&3&1 \\ 1&1&2&3 \\ 3&1&1&2 \end{pmatrix}\ ,\quad A_1 = \begin{pmatrix} 1&6&8&4 \\ 4&1&6&8 \\ 8&4&1&6 \\ 6&8&4&1 \end{pmatrix}\ ,\quad A_2 = \begin{pmatrix} 1&9&4&\mathtt{a} \\ \mathtt{a}&1&9&4 \\ 4&\mathtt{a}&1&9 \\ 9&4&\mathtt{a}&1 \end{pmatrix}\ .$$

Table 2. Lower Bounds of Number of Active S-boxes and Weights of Characteristics

	F64A							F64B		
round	Dif.	DP_{max} 2^{-6}	DP_{max} 2^{-5}	Lin.	LP_{max} 2^{-6}	LP_{max} $2^{-4.39}$	speed (cycles/byte)	Dif.	Lin.	speed (cycles/byte)
1	**0**	0	0	**0**	0	0	-	**0**	**0**	-
2	**1**	6	5	**1**	6	4.39	-	**1**	**1**	-
3	**2**	12	10	**5**	30	21.95	-	**2**	**5**	-
4	**5**	30	25	**5**	30	21.95	-	**5**	**5**	-
5	**6**	36	30	**6**	36	26.34	-	**6**	**6**	-
6	**10**	60	50	**10**	60	43.9	-	**10**	**10**	-
7	**10**	60	50	**10**	60	43.9	-	**10**	**10**	-
8	**11**	66	55	**11**	66	48.29	-	**11**	**11**	-
9	**12**	72	60	**15**	80	65.85	-	**15**	**15**	-
10	**15**	80	75	**15**	80	65.85	17.52	**15**	**15**	17.53
11	**16**	86	80	**16**	86	70.24	-	**16**	**16**	-
12	**20**	120	100	**20**	120	87.8	20.52	**20**	**20**	20.52
13	**20**	120	100	**20**	120	87.8	-	**20**	**20**	-
14	**21**	126	105	**21**	126	92.19	23.66	**21**	**21**	23.66
15	**22**	132	110	**25**	130	109.75	-	**25**	**25**	-
16	**25**	150	125	**25**	130	109.75	26.17	**25**	**25**	26.17
17	**26**	156	130	**26**	136	114.14	-	**26**	**26**	-
18	**30**	180	150	**30**	180	131.7	29.03	**30**	**30**	29.03

Let A'_0, A'_1 and A'_2 be 32×32 matrices over $GF(2)$ which are equivalent to A_0, A_1 and A_2, respectively. These matrices have the following branch number properties.

1. $\mathcal{B}r_8(A'_0) = \mathcal{B}r_8(A'_1) = \mathcal{B}r_8(A'_2) = 5$,
2. $\mathcal{B}r_8([A'_0|A'_1]) = \mathcal{B}r_8([A'_1|A'_2]) = \mathcal{B}r_8([A'_2|A'_0]) = 5$,
3. $\mathcal{B}r_8([A'_0|A'_1|A'_2]) = 5$,
4. $\mathcal{B}r_8([{}^tA'^{-1}_0|{}^tA'^{-1}_1]) = \mathcal{B}r_8([{}^tA'^{-1}_1|{}^tA'^{-1}_2]) = \mathcal{B}r_8([{}^tA'^{-1}_2|{}^tA'^{-1}_0]) = 5$.

Contrary to the 8×8 matrices cases, all of these conditions indicate that the branch numbers are optimal. Note that we chose the matrix A_0 is from AES/Rijndael's diffusion matrix for reference [5].

Let F64A and F64B be a $(4, 8, 2r)$-SPFS which employs the matrices A_0, A_1 and A_2 same as in F128A and F128B, respectively. F64A and F64B can be used for 64-bit blockciphers. The lower bounds of active S-boxes indicated by our theory and weight of the characteristics are shown in Table 2.

We evaluate software performance (in cycles per byte) of a moderately optimized C implementation of the F64A and F64B are measured on an AMD Athlon64 4000+ (2.41GHz) with Windows XP Professional x64 Edition and Visual Studio .NET 2003 (same as Table 1 environment). We confirmed that they achieve practically enough speed in this environment. Moreover we expect that F64A and F64B can be implemented efficiently on 32-bit processors, because they require smaller tables than F128A and F128B do.