On Feistel Ciphers using Optimal Diffusion Mappings across Multiple Rounds

Taizo Shirai[1]* and Bart Preneel[2]

[1]Sony Corporation, Tokyo, Japan
taizo.shirai@jp.sony.com
[2]ESAT/SCD-COSIC, Katholieke Universiteit Leuven, Belgium
bart.preneel@esat.kuleuven.ac.be

Abstract. We study a recently proposed design approach of Feistel ciphers which employs optimal diffusion mappings across multiple rounds. This idea was proposed by Shirai and Shibutani at FSE2004, and the technique enables to improve the immunity against either differential *or* linear cryptanalysis (but not both). In this paper, we present a theoretical explanation why the new design using three different matrices achieves the better immunity. In addition, we are able to prove conditions to improve the immunity against both differential *and* linear cryptanalysis. As a result, we show that this design approach guarantees at least $R(m+1)$ active S-boxes in $3R$ consecutive rounds ($R \geq 2$) where m is the number of S-boxes in a round. By using the guaranteed number of active S-boxes, we compare this design approach to other well-known designs employed in SHARK, Rijndael, and MDS-Feistel ciphers. Moreover, we show interesting additional properties of the new design approach.

Keywords optimal diffusion mapping, Feistel cipher, active S-boxes, MDS

1 Introduction

A Feistel structure is one of the most widely used and best studied structures for the design of block ciphers. It was first proposed by H. Feistel in 1973; subsequently the structure was adopted in the well-known block cipher DES [5,6]. The main advantage of the Feistel structure is its involution property, which provides flexible designs of the underlying F-functions. During the 30 year history of modern block ciphers, extensive studies have been made on Feistel structure [8, 11, 14]. Currently, many well-known block ciphers, e.g. Camellia [1], Misty [10], RC6 [13], Twofish [15], employed the design of Feistel structures.

Recently, Shirai and Shibutani proposed a novel design approach of Feistel ciphers based on the concept of optimal diffusion mappings [18]. An optimal diffusion is a linear function with maximum branch number; the concept of optimal diffusion is used in the design of AES and many other cryptographic primitives [2, 4, 12, 15]. From their empirical analytic results, the immunity against

* A guest researcher at ESAT/SCD-COSIC, K.U.Leuven from 2003 to 2004.

either differential and linear cryptanalysis (but not both) would be strengthened significantly if the linear diffusion layer of the Feistel structure satisfies special optimal diffusion conditions across multiple rounds. In this way difference cancellation in the Feistel structure caused by a small number of active S-boxes will not occur. This result opened a new line of research on the Feistel structure. A theoretical proof of the effectiveness of the proposed design and a solution to improve the immunity against both differential *and* linear cryptanalysis remained unsolved.

In this paper, we will call the *"Optimal Diffusion Mappings across Multiple Rounds"* design approach of Feistel ciphers the *ODM-MR design*. Our contribution is that we first give a theoretical explanation of the effectiveness of the *ODM-MR design* implied by Shirai and Shibutani. Second, we found new conditions and proofs to improve the immunity of both differential *and* linear cryptanalysis. Let m be the number of S-boxes in an F-function. As a result, by combining previous and novel conditions, we finally show that Feistel ciphers with the *ODM-MR design* guarantees $R(m+1)$ active S-boxes in $3R$ consecutive rounds for $R \geq 2$.

In order to further investigate the properties of the *ODM-MR design*, we compare the ratio of guaranteed active S-boxes to all employed S-boxes of the *ODM-MR design* to other design approaches employed in MDS-Feistel, SHARK and AES/Rijndael. All of them use optimal diffusion mappings in their linear diffusion. Consequently, in 128-bit block and 8-bit S-box settings, we obtain a limit of 0.371 for the active S-box ratio of *ODM-MR design* when the number r of rounds goes to infinity, which means that we can guarantee 37.1% active S-boxes with this design strategy. This result is apparently better than MDS-Feistel's ratio of 0.313. Moreover we show that for the number of S-boxes in an F-function and the round number go to infinity, the converged ratio of *ODM-MR* is 0.333. This is better than Rijndael-type diffusion layer's ratio 0.250. From these limit values, we can conclude that *ODM-MR* performs better than the other approaches in certain settings.

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 theorems regarding *ODM-MR* as our main contribution. In Sect. 5, we discuss the new design by presenting some numerical values. Finally Sect. 6 concludes the paper. The method to construct the concrete Feistel ciphers with *ODM-MR design* is proposed in Appendix A.

2 Preliminaries

In this paper, we treat the typical Feistel structure, which is called a balanced Feistel structure. It is defined as follows [14].

Definition 1. *(Balanced Feistel structure)*
Let $E : \{0,1\}^b \times \{0,1\}^k \rightarrow \{0,1\}^b$ be a b-bit block cipher (for b even) with a k-bit key. Let r be the number of rounds, $k_i \in \{0,1\}^{k'}$ be the k'-bit round key provided

by a key scheduling algorithm and $x_i \in \{0,1\}^{b/2}$ *be intermediate data, and let* $F_i : \{0,1\}^{k'} \times \{0,1\}^{b/2} \rightarrow \{0,1\}^{b/2}$ *be the F-function of the i-th round. The encryption and decryption algorithm of a balanced Feistel Cipher E are defined as follows*

Algorithm $Feistel.Encrypt_K(P)$	**Algorithm** $Feistel.Decrypt_K(C)$
input $P \in \{0,1\}^b$, $K \in \{0,1\}^k$	**input** $C \in \{0,1\}^b$, $K \in \{0,1\}^k$
$x_0 \leftarrow msb_{b/2}(P)$, $x_1 \leftarrow lsb_{b/2}(P)$	$x_0 \leftarrow msb_{b/2}(C)$, $x_1 \leftarrow lsb_{b/2}(C)$
for $i = 1$ **to** r **do**	**for** $i = 1$ **to** r **do**
$\quad x_{i+1} = F_i(k_i, x_i) \oplus x_{i-1}$	$\quad x_{i+1} = F_i(k_{r-i+1}, x_i) \oplus x_{i-1}$
$msb_{b/2}(C) \leftarrow x_{r+1}$, $lsb_{b/2}(C) \leftarrow x_r$	$msb_{b/2}(P) \leftarrow x_{r+1}$, $lsb_{b/2}(P) \leftarrow x_r$
return $C \in \{0,1\}^b$	**return** $P \in \{0,1\}^b$

where $msb_x(y)$ $(lsb_x(y))$ *represents the most (least) significant x-bit of y.*

Then we define SP-type F-functions which are a special type of F-function constructions [7, 17].

Definition 2. *(SP-type F-function)*
Let the length of 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 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 define the intermediate variables* $z_i = S_i(x_i \oplus k_i)$.

Definition 3. *((m,n,r)-SPMFC)*
An (m, n, r)*-SPMFC is defined as an r-round Feistel cipher 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 *of* (m, n, r)*-SPMFC.*

We also give definitions of bundle weight and branch number [4].

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

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

Definition 5. *(Branch Number)*
Let $\theta : \{0,1\}^{kn} \rightarrow \{0,1\}^{ln}$. *The branch number of* θ *is defined as*

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

Remark 1. The maximum branch number is $\mathcal{B}(\theta) = l+1$. 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 codes known as MDS codes [4].

3 Previous Work

The precise estimation of the lower bound of the number of active S-boxes of block ciphers has been known as one of the practical means to evaluate ciphers, because this lower bound can be used to calculate the upper bound of the differential characteristic probability or the linear characteristic probability [1,3,4,7,9,17]. Shimizu has shown a conjectured lower bound of the number of differentially and linearly active S-boxes for certain (m, n, r)-SPMFC block ciphers, in which a unique optimal diffusion mapping is repeatedly used in all F-functions [16]. Since such optimal diffusion mappings can be obtained from a generation matrix of an MDS code, we call the design MDS-Feistel [2,4,18].

Shimizu showed the following formula.

Conjecture 1. Let A be an $mn \times mn$ matrix over $GF(2)$ of an optimal diffusion mapping with maximum branch number $m+1$. Let E be an (m, n, r)-SPMFC block cipher and all matrices of diffusion layers are represented by the unique matrix $M_i = A$ $(1 \leq i \leq r)$. Then a lower bound of the differentially and linearly active S-boxes of E is conjectured as

$$L(r) = \lfloor r/4 \rfloor (m+2) + (r \mod 4) - 1 \ . \quad (1)$$

In Table 1, the columns indicated by 'M1' show the conjectured lower bounds of number of active S-boxes, and the data of the conjectured values are plotted on the left side of Fig. 3. This simple relation between the round number and the guaranteed number of active S-boxes is considered as a useful tool for evaluating similar kinds of block cipher designs. While this conjecture has not been proved, empirically, it has been partially confirmed [18].

Recently, at FSE 2004, Shirai and Shibutani proposed a novel design approach to improve the minimum number of active S-boxes of Feistel ciphers by employing optimal diffusion mappings across multiple round functions, the *ODM-MR design* approach [18]. By carefully analyzing the difference cancellations, they found the following properties:

Property 1. Let E be an (m, n, r)-SPMFC block cipher.

- For matrices M_i $(1 \leq i \leq r)$, if every concatenation of two matrices M_j and M_{j+2} for all possible j, denoted by $[M_j | M_{j+2}]$, is an optimal diffusion mapping, the minimum number of differentially active S-boxes is increased from an MDS-Feistel cipher.

- Additionally, if each concatenation of three matrices M_j, M_{j+2} and M_{j+4} for all possible j, denoted by $[M_j|M_{j+2}|M_{j+4}]$, is an optimal diffusion mapping, the minimum number of differentially active S-boxes is increased further than when only satisfying the above conditions on two matrices.
- Even if the number of concatenated matrices is larger than 3, no explicit gain of the number of active S-boxes has been observed in their simulations.

These results imply that by avoiding a linear correlation between F-functions in round $(i, i+2)$ or rounds $(i, i+2, i+4)$, the *ODM-MR* construction guarantees more active S-boxes.

In Table 1, the columns indicated by 'D' show the result of the improved minimum number of differentially active S-boxes when every concatenated matrix of three matrices $[M_i|M_{i+2}|M_{i+4}]$ is an optimal diffusion mapping. The graph of the corresponding values are shown on the left side of Fig. 2.

This result opened a new line of research on developing more efficient Feistel ciphers. On the other hand a theoretical justification of the gain of the proposed construction and an explicit method to improve the immunity against both differential *and* linear cryptanalysis remained unsolved.

4 Proofs of Effectiveness of the *ODM-MR Design*

In this section, we provide the first proofs for the effectiveness of the *ODM-MR design* using three different matrices. We also show an additional condition and some proofs in order to improve the lower bound of linearly active S-boxes by using two different matrices. Our main contribution is to show the following corollary which presents a simple relation between the number of rounds and the guaranteed numbers of active S-boxes in the *ODM-MR design*. In the corollary, note that ${}^tM$ denotes the transpose matrix of a matrix M.

Corollary 1. *Let E be a (m,n,r)-SPMFC block cipher 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 $R(m+1)$ differentially and linearly active S-boxes.*

Fig. 1 illustrates the statement of the corollary. By using the Corollary 1, we can guarantee theoretically arbitrary number of active S-boxes by increasing the number of rounds. Since the corollary can be immediately obtained from two theorems, i.e. Theorem 1 and Theorem 2, the following two subsections are devoted to the proofs of these theorems. To ease the proofs, we first introduce an additional definition.

Definition 6. *Consider a differential characteristic or linear approximation. Let D_i and L_i denote the number of differentially and linearly active S-boxes in the i-th round, respectively. These values are determined by the difference $\Delta x_i, \Delta z_i$ or by the linear mask $\Gamma x_i, \Gamma z_i$ as follows.*

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

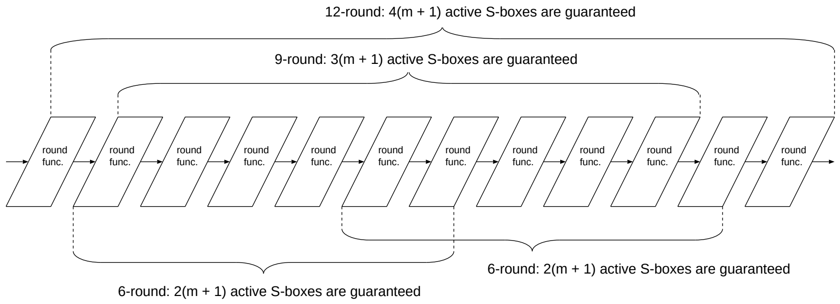

Fig. 1. Guaranteed Active S-boxes by *ODM-MR design*

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

Remark 2. Note that a given difference characteristic always contains a nonzero input difference, since any (m, n, r)-SPMFC's F-functions are bijective. Hence we obtain the following conditions:

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

Since a linear approximation always contains a nonzero input mask, we obtain

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

4.1 Proofs for the Lower Bound of Differentially Active S-boxes

In this section we prove Theorem 1; the proof is based on five lemmata.

Lemma 1 shows relations between D_i of (m, n, r)-SPMFC when every M_i is an optimal diffusion mapping.

Lemma 1. *Let E be an (m, n, r)-SPMFC block cipher. If every M_i has maximum branch number $m + 1$, then E satisfies the following condition $(d2)$.*

$$(d2) \quad D_{i+1} \neq 0 \Rightarrow D_i + D_{i+1} + D_{i+2} \geq m + 1 \ .$$

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 maximum branch number $m + 1$ we have

$$w_n(\Delta z_{i+1}) \neq 0 \Rightarrow w_n(\Delta z_{i+1}) + w_n(\Delta x_i \oplus \Delta x_{i+2}) \geq m + 1 \ . \qquad (2)$$

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

Remark 3. By combining Remark 2 and $(d2)$, we can obtain additional underlying conditions $(d3)$ and $(d4)$.

$$\begin{array}{ll}(d3) & D_i = 0, \Rightarrow D_{i+1} + D_{i+2} \geq m+1 \ , \\ (d4) & D_{i+2} = 0, \Rightarrow D_i + D_{i+1} \geq m+1 \ .\end{array}$$

Equations $(d3)$ and $(d4)$ mean that if round k has no active S-boxes, any 2 consecutive rounds next to round k always contain more than $m+1$ active S-boxes.

Next, we show the property of (m,n,r)-SPMFC in which every $[M_i|M_{i+2}]$ is an optimal diffusion mapping. This is true for the *ODM-MR*.

Lemma 2. *Let E be a (m,n,r)-SPMFC block cipher. If every* $[M_i|M_{i+2}]$ *has maximum branch number* $m+1$*, E satisfies the following conditions* $(d5), (d6)$*.*

$$\begin{array}{ll}(d5) & D_{i+4} = 0 \Rightarrow D_i + D_{i+1} + D_{i+3} \geq m+1 \ , \\ (d6) & D_i = 0 \Rightarrow D_{i+1} + D_{i+3} + D_{i+4} \geq m+1 \ .\end{array}$$

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 maximum branch number $m+1$, and from Remark 2, we see that $w_n(\Delta z_{i+1}) = 0$ and $w_n(\Delta z_{i+3}) = 0$ will never occur simultaneously, we obtain

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

By 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 lemma for the guaranteed number of differentially active S-boxes of (m,n,r)-SPMFC.

Lemma 3. *Let E be a (m,n,r)-SPMFC block cipher where* $r \geq 6$*. If every* $[M_i|M_{i+2}]$ *is an optimal diffusion mapping, then any* 6 *consecutive rounds in E guarantee at least* $2(m+1)$ *differentially 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 $D_i+D_{i+1}+D_{i+2} \geq m+1$ and $D_{i+3}+D_{i+4}+D_{i+5} \geq m+1$. Therefore we obtain $\sum_{k=i}^{i+5} D_k \geq 2(m+1)$. 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),

$$\sum_{k=i}^{i+5} D_k \geq (m+1) + (m+1) = 2(m+1) \ .$$

The case of $D_{i+4} = 0$ is proven similarly from $(d1)$, $(d4)$ and $(d5)$. □

Next, we show the property of an (m, n, r)-SPMFC in which every $[M_i|M_{i+2}|M_{i+4}]$ has maximum branch number. This coincides with one of the *ODM-MR design*.

Lemma 4. *Let E be a (m,n,r)-SPMFC block cipher. If every $[M_i|M_{i+2}|M_{i+4}]$ is an optimal diffusion mapping, then E satisfies the following condition $(d7)$.*

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

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 maximum branch number, and from Remark 2, $w_n(\Delta z_{i+1})$, $w_n(\Delta z_{i+3})$, and $w_n(\Delta z_{i+5})$ cannot be simultaneously 0, we get that

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

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 lemma.

Lemma 5. *Let E be a (m,n,r)-SPMFC block cipher where $r \geq 9$. If every $[M_i|M_{i+2}|M_{i+4}]$ is an optimal diffusion mapping, then any 9 consecutive rounds in E guarantee at least $3(m+1)$ differentially 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 $D_i + D_{i+1} + D_{i+2} \geq m+1$ from (d2), and Lemma 3 guarantees that the sum of the remaining 6 consecutive rounds is equal to $\sum_{k=i+3}^{i+8} D_k \geq 2(m+1)$. Consequently $\sum_{k=i}^{i+8} D_k \geq 3(m+1)$. Similarly, if $D_{i+7} \neq 0$, at least $3(m+1)$ 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),

$$\sum_{k=i}^{i+8} D_k \geq (m+1) + (m+1) + (m+1) = 3(m+1) \ .$$

As a consequence, we have shown that any 9 consecutive rounds of E guarantee at least $3(m+1)$ differentially active S-boxes. □

We conclude this section with

Theorem 1. *Let E be an (m,n,r)-SPMFC block cipher where $r \geq 6$. If every $[M_i|M_{i+2}|M_{i+4}]$ is an optimal diffusion mapping, any $3R$ consecutive rounds in E guarantees at least $R(m+1)$ differentially active S-boxes.*

Proof. Any integer $3R$ $(R \geq 2)$ can be written as $3R = 6k + 9j$ $(k + j \geq 1, 2k + 3j = R)$. From lemmata 3 and 5, 6 and 9 consecutive rounds of E guarantee $2(m+1)$ and $3(m+1)$ differentially active S-boxes, respectively. Therefore, E guarantees $k * 2(m+1) + j * 3(m+1) = (2k+3j)(m+1) = R(m+1)$ differentially active S-boxes. □

4.2 Proofs for the Lower Bound of Linearly Active S-boxes

In this subsection, we will show the proof of the guaranteed number of linearly active S-boxes of (m,n,r)-SPMFC with *ODM-MR design.*

Theorem 2. *Let E be an (m, n, r)-SPMFC block cipher. If every $[{}^tM_i^{-1}|{}^tM_{i+2}^{-1}]$ is an optimal diffusion mapping for any i, any $3R$ consecutive rounds in E has at least $R(m+1)$ linearly 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 maximum branch number $m+1$, and from Remark 2, $w_n(\Gamma z_i)$ and $w_n(\Gamma z_{i+2})$ cannot be simultaneously 0, we obtain

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

By using the notion of L_i, this implies,

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

This shows that every 3 consecutive rounds guarantees at least $m+1$ linearly active S-boxes. Consequently, any $3R$ consecutive rounds in E guarantees $\sum_{k=i}^{i+3R-1} L_k \geq R(m+1)$. □

Finally, by simply combining Theorems 1 and 2, the claimed Corollary 1 follows directly. Appendix A contains example matrices that satisfy the *ODM-MR design*.

5 Discussion

5.1 Comparison of *ODM-MR* and MDS-Feistel

To discuss the implications of this new design approach, we show empirical search results for the cases $r = 12, m = 4, .., 8$. To obtain these results we employed a weight based search method. This approach has been used by Shirai and Shibutani before [18]. Our results are shown in Table 1. In the table, the values for more than 13-rounds are interpolated by the corollary and Shimizu's conjecture. Note that the simulation results completely match the lower bound values predicted by the corollary, which are denoted by the underlined values. These results show the superiority of *ODM-MR design* over MDS-Feistel explicitly.

Fig. 2 shows graphs of the results in Table 1, and five auxiliary lines $y = (m+1)x/3$ are added where $m = 4, .., 8$. These lines connect the lower bounds values of every $3R$-round.

The left side of Fig. 3 shows an estimated lower bound of MDS-Feistel and approximate lines $y = (m+2)x/4-1$. To see the effect of the *ODM-MR* approach graphically, the right side of Fig. 3 includes the approximated lines for *ODM-MR* and MDS-Feistel for $m = 4$ and $m = 8$. The differences of the gradients show explicitly the advantage of the *ODM-MR* approach.

Table 1. Lower Bounds of MDS-Feistel and *ODM-MR design*

	$m=4$			$m=5$			$m=6$			$m=7$			$m=8$		
Round	M1	D	L	M1	D	L	M1	D	L	M1	D	L	M1	D	L
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	2	2	5	2	2	6	2	2	7	2	2	8	2	2	9
4	5	5	5	6	6	6	7	7	7	8	8	8	9	9	9
5	6	6	6	7	7	7	8	8	8	9	9	9	10	10	10
6	7	10	10	8	12	12	9	14	14	10	16	16	11	18	18
7	8	10	10	9	12	12	10	14	14	11	16	16	12	18	18
8	11	12	11	13	14	13	15	16	15	17	18	17	19	20	19
9	12	15	15	14	18	18	16	21	21	18	24	24	20	27	27
10	13	16	15	15	18	18	17	22	21	19	24	24	21	28	27
11	14	17	16	16	20	19	18	23	22	20	26	25	22	29	28
12	17	20	20	20	24	24	23	28	28	26	32	32	29	36	36
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
15	20	**25**	**25**	23	**30**	**30**	26	**35**	**35**	29	**40**	**40**	32	**45**	**45**
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
18	25	**30**	**30**	29	**36**	**36**	33	**42**	**42**	37	**48**	**48**	41	**54**	**54**

M1: numbers of active S-boxes of MDS-Feistel
D: numbers of differentially active S-boxes of *ODM-MR*
L: numbers of linearly active S-boxes of *ODM-MR*

5.2 Active S-box Ratio

In this subsection, we compare the *ODM-MR* approach to other design approaches using the new type of approach. Since we obtained a formal bound for the lower bound of the *ODM-MR design* approach, we can compare it to other well known design approaches based on the concept of active S-box ratio introduced by Shirai and Shibutani [18].

Let $active(r,m)$ be the number of guaranteed active S-boxes for an r-round cipher which employs $m \times m$ diffusion matrices over $GF(2^n)$ in its diffusion layer. For example, $active(r,m)$ of the MDS-Feistel design can be written as

$$active(r,m) = (m+2)\lfloor r/4 \rfloor + \alpha_{r,m} \ ,$$

where $\alpha_{r,m} = (r \mod 4) - 1$. Generally, $\alpha_{r,m}$ is a function which maximum absolute value is proportional to m and $lim_{r\to\infty}\alpha_{r,m}/r = 0$.

Next, let $total(r,m)$ be the total number of S-boxes in an r-round cipher. The ratio of the number of active S-boxes to the total number of S-boxes becomes

$$ratio(r,m) = \frac{active(r,m)}{total(r,m)} = \frac{(m+2)\lfloor r/4 \rfloor + \alpha_{r,m}}{rm} \ .$$

By using the definition of active S-box ratio, we can study the characteristic of the MDS-Feistel design. For example, consider a 128-bit block cipher employing

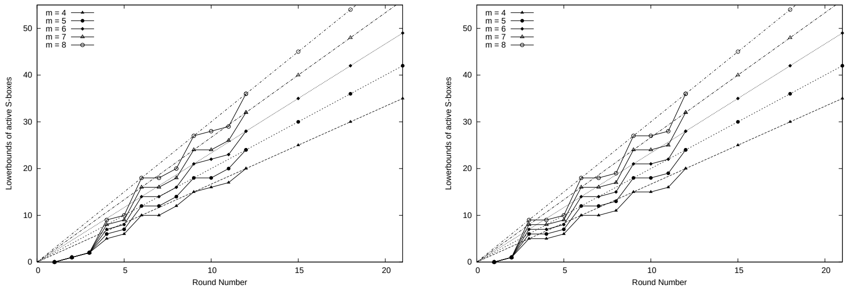

Fig. 2. Lower bounds of the *ODM-MR design* ($m = 8$)

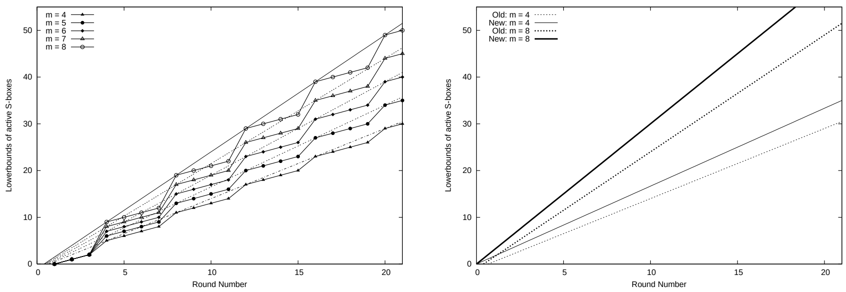

Fig. 3. Comparison of MDS-Feistel and *ODM-MR design*

8-bit S-boxes. For $m = 8$, $ratio(r, 8)$ will converge to a specific value when r goes to infinity,

$$\lim_{r\to\infty} ratio(r, 8) = \lim_{r\to\infty} \frac{10\lfloor r/4\rfloor + \alpha_{r,8}}{8r} = \frac{10}{32} = 0.3125 \ .$$

This implies that about 31% of all S-boxes will be active for a very large number of rounds. This limit can be considered as a potentially guaranteed ratio of active S-boxes corresponding to the chosen m.

Also, we can take the limit of $ratio(r, m)$ when both r and m tend to infinity,

$$\lim_{r,m\to\infty} ratio(r, m) = \frac{(m + 2)\lfloor r/4\rfloor + \alpha_{r,m}}{rm} = \frac{1}{4} = 0.25 \ .$$

Even though huge r and m are not practical in the real world, the value can be understood as an indicator of the potential efficiency of a particular design strategy.

We propose these limits as a reference to evaluate the efficiency of the linear diffusion layer of the cipher and use them to compare ciphers employing different design strategies. The following table contains the convergence values of the "MDS-Feistel" and the"*ODM-MR*" design. Additionally, the following "Rijndael type" and "SHARK type" design approaches are also evaluated for reference.

Rijndael type: A nm^2-bit SPN block cipher design whose round function consists of key-addition, $m \times m$ parallel n-bit S-boxes, a MixColumn employing m $m \times m$ matrices over $GF(2^n)$ and a ShiftRow operation [4].

SHARK type: A nm-bit SPN block cipher design where m parallel n-bit S-boxes, an $m \times m$ matrix over $GF(2^n)$ are employed [12].

Type	$active(r,m)$	$total(r,m)$	128bit blk.	$\lim_{r\to\infty}$	$\lim_{m,r\to\infty}$
MDS-Feistel	$(m+2)\lfloor r/4 \rfloor + \alpha_{r,m}$	rm	$m = 8$	0.313	0.25
ODM-MR	$(m+1)\lfloor r/3 \rfloor + \beta_{r,m}$	rm	$m = 8$	0.371	0.33
Rijndael type	$(m+1)^2\lfloor r/4 \rfloor + \gamma_{r,m}$	rm^2	$m = 4$	0.391	0.25
SHARK type	$(m+1)\lfloor r/2 \rfloor + \theta_{r,m}$	rm	$m = 16$	0.531	0.5

Table 2. Comparison of the Active S-box Ratio

Note that all four designs employ optimal diffusion mappings in their diffusion layers; they have block length of 128 bits with 8-bit S-boxes. The result shows that the *ODM-MR* approach has the better limit than MDS-Feistel in the 128-bit block setting which is also confirmed by the empirical results in the previous section. We also know that *ODM-MR*'s limit is closer to that of the Rijndael design approach than MDS-Feistel.

Moreover, the limit value of the *ODM-MR* approach, when both r and m tend to infinity, exceeds that of the Rijndael type construction. This is due to the fact that the *ODM-MR* approach guarantees a certain number of active S-boxes for 3 consecutive rounds, while the Rijndael-type approach has such a property for 4 consecutive rounds.

The values of SHARK are still the highest, because the design strategy has a 2-round property. However, there seems to be a tradeoff for the implementation cost, as SHARK-type design requires matrices which are twice as large as the matrices in the MDS-Feistel and *ODM-MR* and four times as large as in the Rijndael approach.

6 Conclusion

We provide a theoretical motivation for the *ODM-MR design*. We first give a theoretical reason of *ODM-MR*, and found additional conditions and proofs to improve the immunity against differential *and* linear cryptanalysis. As a result, we showed that the *ODM-MR design* approach guarantees at least $R(m+1)$ active S-boxes in $3R$ consecutive rounds ($R \geq 2$) where m is the number of S-boxes in a round. This guaranteed number of active S-boxes was compared with the design approach of other well-known designs namely SHARK, Rijndael, and MDS-Feistel ciphers. We were able to show that our design approach outperforms some of the other designs.

Acknowledgments We thank An Braeken and Christopher Wolf for carefully reading the earlier version of the paper. We thank the anonymous referees for helpful 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, *The Design of Rijndael: AES - The Advanced Encryption Standard (Information Security and Cryptography)*. Springer, 2002.
5. H. Feistel, "Cryptography and computer privacy." *Scientific American*, vol. 228, pp. 15–23, May 1973.
6. Data Encryption Standard, "Federal Information Processing Standard (FIPS)." National Bureau of Standards, U.S. Department of Commerce, Washington D.C., Jan. 1977.
7. 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.
8. M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions." *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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/.
14. 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.
15. 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/.

16. H. Shimizu, "On the security of Feistel cipher with SP-type F function." in *Proceedings of SCIS – SCIS 2001*, 2001.
17. 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.
18. 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

We show one of methods to construct a Feistel cipher satisfying the *ODM-MR design*. To construct a concrete cipher, at least three $m \times m$ matrices over $GF(2^n)$ are required to satisfy all the *ODM-MR* conditions. The construction steps are:

1. Choose $m \times m$ matrices A_0, A_1, A_2 over $GF(2^n)$ such that,
   (a) Every square submatrix of $[A_0|A_1|A_2]$ is nonsingular,
   (b) Every square submatrix of $\left[\frac{A_0^{-1}}{A_1^{-1}}\right]$, $\left[\frac{A_1^{-1}}{A_2^{-1}}\right]$ and $\left[\frac{A_2^{-1}}{A_0^{-1}}\right]$ is nonsingular.
2. Set these three matrices as $M_{2i+1} = M_{2r-2i} = A_{\ i \ mod \ 3}$, for $(0 \leq i < r)$ in a Feistel cipher with $2r$ rounds.

Note that all operations in Step 1 are over $GF(2^n)$ although the optimal diffusion conditions for $[M_i M_{i+2} M_{i+4}]$ and $[{}^tM_j^{-1} {}^tM_{j+2}^{-1}]$ are given over $GF(2)$.

Here we show an example of three matrices A_0, A_1, A_2 for the case $m = 4$.

Example 1. The following matrices A_0, A_1, A_2 satisfy the *ODM-MR* conditions.

$$A_0 = \begin{pmatrix} \texttt{9d} & \texttt{b4} & \texttt{d3} & \texttt{5d} \\ \texttt{29} & \texttt{34} & \texttt{39} & \texttt{60} \\ \texttt{67} & \texttt{6a} & \texttt{d2} & \texttt{e3} \\ \texttt{8e} & \texttt{d7} & \texttt{e6} & \texttt{1b} \end{pmatrix}, \quad A_1 = \begin{pmatrix} \texttt{ae} & \texttt{ec} & \texttt{b9} & \texttt{3e} \\ \texttt{81} & \texttt{25} & \texttt{13} & \texttt{d4} \\ \texttt{db} & \texttt{9d} & \texttt{4} & \texttt{1b} \\ \texttt{9e} & \texttt{3a} & \texttt{91} & \texttt{39} \end{pmatrix}, \quad A_2 = \begin{pmatrix} \texttt{b8} & \texttt{f1} & \texttt{65} & \texttt{ef} \\ \texttt{3a} & \texttt{f6} & \texttt{2d} & \texttt{6a} \\ \texttt{4a} & \texttt{97} & \texttt{a3} & \texttt{b9} \\ \texttt{82} & \texttt{5f} & \texttt{a2} & \texttt{c1} \end{pmatrix}.$$

Each element is expressed as hexadecimal value corresponding to a binary representation of elements in $GF(2^8)$ with a primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. From the corollary, a $(4, 8, 12)$-SPNFC employing the above matrices A_0, A_1, A_2 as outlined in Fig. 4 guarantees 10, 15 and 20 differentially and linearly active S-boxes in 6, 9 and 12 consecutive rounds, respectively.

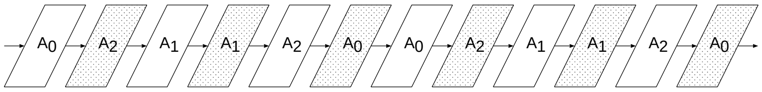

Fig. 4. Example Allocation of Matrices A_0, A_1, A_2