Provable Security against Differential and Linear Cryptanalysis for the SPN Structure

Seokhie Hong[1]*, Sangjin Lee, Jongin Lim, Jaechul Sung, Donghyeon Cheon, and Inho Cho

Center for Information and Security Technologies(CIST),
Korea University, Seoul, KOREA,
hsh@semi.korea.ac.kr

Abstract. In the SPN (Substitution-Permutation Network) structure, it is very important to design a diffusion layer to construct a secure block cipher against differential cryptanalysis and linear cryptanalysis. The purpose of this work is to prove that the SPN structure with a maximal diffusion layer provides a provable security against differential cryptanalysis and linear cryptanalysis in the sense that the probability of each differential (respectively linear hull) is bounded by p^n (respectively q^n), where p (respectively q) is the maximum differential (respectively liner hull) probability of n S-boxes used in the substitution layer. We will also give a provable security for the SPN structure with a semi-maximal diffusion layer against differential cryptanalysis and linear cryptanalysis.

1 Introduction and Motivation

The Feistel structure has been used widely in the iterated block cipher. In this structure, the input to each round is divided into two halves. The right half is transformed by some nonlinear function and then xored to the left half and the two halves are swapped except for the last round. On the other hand, the SPN structure is designed using round function on the whole data block. Nowadays, the SPN structure is also attracting interest because it is highly parallelizable and easy to analyze the security against differential cryptanalysis(DC) and linear cryptanalysis(LC).

The most well known attacks on block ciphers are DC[1,2,3] and LC[6,7]. In DC, one uses characteristic which describes the behavior of input and output differences for some number of consecutive rounds. But it may not be necessary to fix the values of input and output differences for the intermediate rounds in a characteristic, so naturally the notion of differential was introduced[15]. The same statements can be applied to LC, so that of linear hull was introduced[11]. However it seems computationally infeasible to compute the maximum probabilities of differential and linear hull if the number of rounds increases.

* The authors wish to acknowledge the financial support of the Korea Research Foundation made in the program year of 1998.

B. Schneier (Ed.): FSE 2000, LNCS 1978, pp. 273–283, 2001.

In [9], K. Nyberg and L.R. Knudsen showed that the r-round differential probability is bounded by $2p^2$ if the maximal differential probability of round function is p and $r \geq 4$. Furthermore, the probability can be reduced to p^2 if the round function is bijective. These results provide a provable security for the Feistel structure against DC. M. Matsui proposed a new block cipher of a Feistel network, MISTY[8] for which security can be shown by the existing results for Feistel structures. The round function of MISTY is itself a Feistel network which is proven secure. From this round function with small S-boxes, he provided sufficiently large and strong S-boxes with proven security.

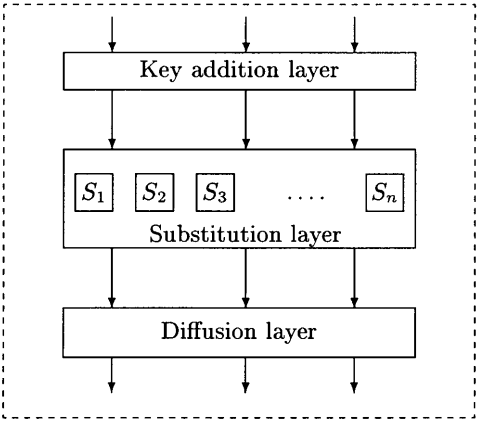

Fig. 1. One round of a SPN structure

In the SPN structure the diffusion layer provides an avalanche effect, both in the contexts of differences and linear approximation, so the notion of branch number was introduced[16]. The branch number of a diffusion layer has been determined to be very important. A cipher with the low branch number may have a fatal weakness even though a substitution layer consists of S-boxes resistant against DC and LC. In this paper we will give a provable security for the SPN structure with a maximal branch number by theorem 1.

This paper proceeds as follows; In section 2 we will introduce some notations and definitions. In section 3 a provable security for the SPN structure with a maximal diffusion layer against DC will be given. Provable security against LC will be given in section 4. Other results will be described in section 5.

2 Preliminaries

In this section we define some notations and definitions. Throughout this paper we consider an SPN structure with mn-bit round function. Let S_i be an $m \times m$

bijective S-box, i.e.,

$$S_i \ : \ \mathbb{Z}_2^m \to \mathbb{Z}_2^m \ \ (1 \le i \le n).$$

Definition 1. *For any given $\Delta x, \Delta y, \Gamma x, \Gamma y \in \mathbb{Z}_2^m$, the differential and linear probability of each S_i are defined as follows;*

$$DP^{S_i}(\Delta x \to \Delta y) = \frac{\#\{x \in \mathbb{Z}_2^m | S_i(x) \oplus S_i(x \oplus \Delta x) = \Delta y\}}{2^m}$$

$$LP^{S_i}(\Gamma x \to \Gamma y) = \left(\frac{\#\{x \in \mathbb{Z}_2^m | \Gamma x \cdot x = \Gamma y \cdot S_i(x)\}}{2^{m-1}} - 1 \right)^2$$

where $\Gamma x \cdot x$ denotes the parity of bitwise xor of Γx and x.

Definition 2. *The maximal differential and linear probability of S_i are defined by*

$$DP_{max}^{S_i} = \max_{\Delta x \neq 0, \Delta y} DP^{S_i}(\Delta x \to \Delta y)$$

and

$$LP_{max}^{S_i} = \max_{\Gamma x, \Gamma y \neq 0} LP^{S_i}(\Gamma x \to \Gamma y),$$

respectively.

In general, S_i is called strong if $DP_{max}^{S_i}$ and $LP_{max}^{S_i}$ are small enough and a substitution layer is called strong if $DP_{max}^{S_i}$ and $LP_{max}^{S_i}$ are small enough for all $1 \le i \le n$. Let us denote by p and q the maximal value of $DP_{max}^{S_i}$ and $LP_{max}^{S_i}$ for $1 \le i \le n$, respectively. That is,

$$p = \max_{1 \le i \le n} DP_{max}^{S_i}, \ \ q = \max_{1 \le i \le n} LP_{max}^{S_i}.$$

Even though p and q are small enough, this does not guarantee a secure SPN structure against DC and LC. Hence the role of the diffusion layer is very important. The purpose of the diffusion layer is to provide an avalanche effect, both in the contexts of differences and linear approximations.

Definition 3. *Differentially active S-box is defined as an S-box given a non-zero input difference and linearly active S-box as an S-box given a non-zero output mask value[5].*

The number of differentially active S-boxes has an effect on probabilities of differential characteristics or differentials. Hence the concept of active S-box plays an important role in giving a provable security for the SPN structure. Conversely differentially(resp. linearly) inactive S-boxes have a zero input xor(resp. output mask value). Consequently they have always a zero output xor(resp. input mask value) with probability 1.

Let $x = (x_1, \cdots, x_n)^t \in GF(2^m)^n$ then the Hamming weight of x is denoted by

$$Hw(x) = \#\{i | x_i \neq 0\}.$$

Note "Hamming weight of X" does not count the number of nonzero bits but count the number of non-zero m-bit characters.

Throughout this paper we assume that the round keys, which are xored with the input data at each round, are independent and uniformly random. By assumption on round keys, key addition layer in Fig.1 has no influence on the number of active S-boxes. Now we define a SDS function with three layer of substitution-diffusion-substitution as depicted in Fig.2.

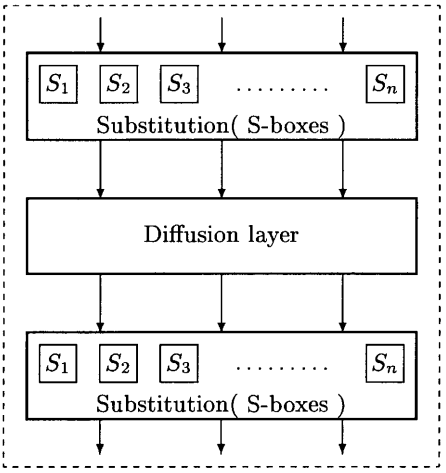

Fig. 2. SDS function

Denote diffusion layer of this SDS function by D, input difference by $\Delta x = x \oplus x^*$, output difference by $\Delta y = y \oplus y^* = D(x) \oplus D(x^*)$, and finally input mask value and output mask values by Γx and Γy, respectively. The minimum number of differentially and linearly active S-boxes of the SDS function are defined as follows;

$$n_d(D) = \min_{\Delta x \neq 0} Hw(\Delta x) + Hw(\Delta y)$$

and

$$n_l(D) = \min_{\Gamma y \neq 0} Hw(\Gamma x) + Hw(\Gamma y),$$

respectively[12]. $n_d(D)$ and $n_l(D)$ are lower bounds for the number of active S-boxes in two consecutive rounds of a differential characteristic and linear approximation, respectively. A diffusion layer is called **maximal** if the $n_d(D)$(equivalently $n_l(D)$) is $n + 1$.

3 Provable Security against DC

In this section we will give a provable security for the SPN structure with a maximal diffusion layer against DC. Throughout this paper we assume that the diffusion layer D of the SDS function can be represented by an $n \times n$ matrix $M = (m_{ij})_{n \times n}$, where $m_{ij} \in GF(2^m)$. That is,

$$M = \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{pmatrix}.$$

J. Daemen et. al [4] showed that, for the diffusion layer D, the relation between input difference(resp. output mask value) and output difference(resp. input mask value) is represented by the matrix M(resp.M^t). That is to say,

$$\Delta y = M\Delta x \ (resp.\ \Gamma x = M^t \Gamma y).$$

So we can redefine $n_d(D)$ and $n_l(D)$ as follows;

$$n_d(D) = \min_{\Delta x \neq 0} \{Hw(\Delta x) + Hw(M\Delta x)\},$$

$$n_l(D) = \min_{\Gamma y \neq 0} \{Hw(\Gamma y) + Hw(M^t \Gamma y)\}.$$

Hence we only need to investigate the matrix M to analyze the role of the diffusion layer D. Let us call M' an $s \times k$ submatrix of M if M' is of the following form;

$$M' = \begin{pmatrix} m_{i_1 j_1} & m_{i_1 j_2} & \cdots & m_{i_1 j_k} \\ m_{i_2 j_1} & m_{i_2 j_2} & \cdots & m_{i_2 j_k} \\ \vdots & \vdots & \ddots & \vdots \\ m_{i_s j_1} & m_{i_s j_2} & \cdots & m_{i_s j_k} \end{pmatrix}$$

Then we say that M contains M' as an $s \times k$ submatrix.

The following lemma shows the necessary and sufficient condition for a diffusion layer to be maximal.

Lemma 1. *Let M be the $n \times n$ matrix representing a diffusion layer D. Then $n_d(D) = n + 1$ if and only if the rank of each $k \times k$ submatrix of M is k for all $1 \leq k \leq n$.*

Proof Assume that $n_d = n + 1$ and there exists a $k \times k$ submatrix M_k of M such that the rank of M_k is less than k for some $1 \leq k \leq n$. Without loss of generality we may assume that

$$M_k = \begin{pmatrix} m_{11} & \cdots & m_{1k} \\ \vdots & \ddots & \vdots \\ m_{k1} & \cdots & m_{kk} \end{pmatrix}.$$

By assumption there exists $(x_1, \cdots, x_k) \neq (0, \cdots, 0)$ such that

$$\begin{pmatrix} m_{11} & \cdots & m_{1k} \\ \vdots & \ddots & \vdots \\ m_{k1} & \cdots & m_{kk} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{1}$$

Let $x = (x_1, \cdots, x_k, 0, \cdots, 0)^t$. By equation (1),

$$Mx = \begin{pmatrix} m_{11} & \cdots & m_{1k} & m_{ik+1} & \cdots & m_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{k1} & \cdots & m_{kk} & m_{kk+1} & \cdots & m_{kn} \\ m_{k+11} & \cdots & m_{k+1k} & m_{k+1k+1} & \cdots & m_{k+1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{n1} & \cdots & m_{nk} & m_{nk+1} & \cdots & m_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \delta_{k+1} \\ \vdots \\ \delta_n \end{pmatrix}. \tag{2}$$

By the definition of $n_d(D)$,

$$n_d(D) \leq Hw(x) + Hw(Mx) \leq k + n - k = n.$$

This is a contradiction to $n_d = n+1$. Therefore we obtained a sufficient condition.

Assume that the rank of each $k \times k$ submatrix of M is k for all $1 \leq k \leq n$ and $n_d < n + 1$. Since $n_d < n + 1$, there exists $x = (x_1, \cdots, x_n)^t \in GF(2^m)^n$ such that

$$Hw(x) + Hw(Mx) \leq n.$$

Without loss of generality we may assume that $x_1, \cdots, x_s$ are all nonzero and $x_j = 0$ for all $j > s$. Let $y = Mx$, then $Hw(y) \leq n - s$. In other words, the number of zero components in y is greater than or equal to s, so we can assume $y_{i_1} = \cdots = y_{i_s} = 0$. We can easily check equation (3).

$$\begin{pmatrix} m_{i_1 1} & \cdots & m_{i_1 s} \\ \vdots & \ddots & \vdots \\ m_{i_s 1} & \cdots & m_{i_s s} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ \vdots \\ y_{i_s} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{3}$$

Hence we can get an $s \times s$ submatrix of M with rank less than s. It is a contradiction to the fact that the rank of each $k \times k$ submatix of M is k for all $1 \leq k \leq n$. ■

In [12], it was shown how a maximal diffusion layer over $GF(2^m)^n$ can be constructed from a maximum distance separable code. If $G_e = [I_{n \times n} B_{n \times n}]$ is the echelon form of the generator matrix of $(2n, n, n + 1)$ RS-code, then

$$\begin{aligned} D : GF(2^m)^n &\to GF(2^m)^n \\ x &\mapsto Bx \end{aligned}$$

is a maximal diffusion layer by lemma 1.

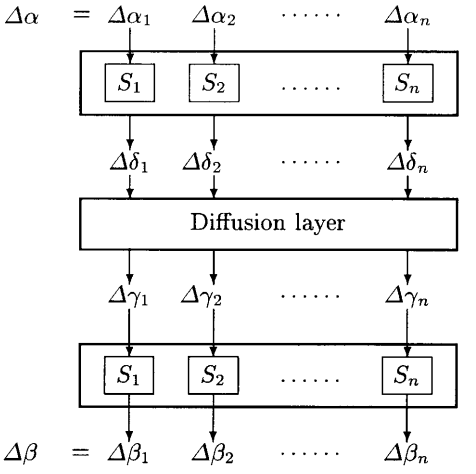

Fig. 3. Differential of SDS function

Consider the differential with input difference $\Delta\alpha = (\Delta\alpha_1, \cdots, \Delta\alpha_n)$ and output difference $\Delta\beta = (\Delta\beta_1, \cdots, \Delta\beta_n)$ as depicted in Fig.3.

Then the probability of this differential is like that;

$$DP(\Delta\alpha \to \Delta\beta) = \sum_{\Delta\delta_1, \cdots, \Delta\delta_n} \left(\prod_{i=1}^{n} DP^{S_i}(\Delta\alpha_i \to \Delta\delta_i) \prod_{i=1}^{n} DP^{S_i}(\Delta\gamma_i \to \Delta\beta_i | \Delta\alpha) \right) \quad (4)$$

Lemma 2. *Let M be the $n \times n$ matrix representing a diffusion layer D and $n_d(D) = n + 1$. In Fig.3, if $Hw(\Delta\alpha) = k$ and $Hw(\Delta\beta) = n - s + 1 (s \leq k)$, there is a index set $\{i_1, \cdots, i_{s-1}\}$ so that $\Delta\alpha_{i_1} \neq 0, \cdots, \Delta\alpha_{i_{s-1}} \neq 0$ and $\{\Delta\delta_{i_1}, \cdots, \Delta\delta_{i_{s-1}}\}$ are determined by the other $\Delta\delta_i$'s.*

Note Since $n_d(D) = n + 1$, s must be less than or equal to k. A index set $\{i_1, \cdots, i_{s-1}\}$ depends on the location of the nonzero $\Delta\alpha$ and $\Delta\beta$.

Proof Without loss of generality we may assume

$$\Delta\beta_1 = 0, \cdots, \Delta\beta_{s-1} = 0 \text{ (or equivalently} \Delta\gamma_1 = 0, \cdots, \Delta\gamma_{s-1} = 0).$$

Let $\Delta\delta' = (\Delta\delta_{i_1} \cdots, \Delta\delta_{i_k})^t$ be the collection of all non-zero components in $\Delta\delta = (\Delta\delta_1, \cdots, \Delta\delta_n)^t$. That is, $\Delta\delta_{i_j} \neq 0$ for all $1 \leq j \leq k$ and $\Delta\delta_t = 0$ if $t \notin \{i_1, \cdots, i_k\}$. Let

$$M' = \begin{pmatrix} m_{1i_1} & \cdots & m_{1i_{s-1}} & m_{1i_s} & \cdots & m_{1i_k} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{s-1i_1} & \cdots & m_{s-1i_{s-1}} & m_{s-1i_s} & \cdots & m_{s-1i_k} \end{pmatrix}.$$

By the definitions of M' and $\Delta\delta'$ and the assumption on $\Delta\beta$, $M'\Delta\delta'$ equals 0. Let's divide $\Delta\delta'$ into two parts, $\Delta\delta_I$ and $\Delta\delta_{II}$, and M' into M_I and M_{II} as followings;

$$\Delta\delta_I = (\Delta\delta_{i_1} \cdots, \Delta\delta_{i_{s-1}})^t,\ \Delta\delta_{II} = (\Delta\delta_{i_s} \cdots, \Delta\delta_{i_k})^t,$$

$$M_I = \begin{pmatrix} m_{1i_1} & \cdots & m_{1i_{s-1}} \\ \vdots & \ddots & \vdots \\ m_{s-1i_1} & \cdots & m_{s-1i_{s-1}} \end{pmatrix} \text{ and } M_{II} = \begin{pmatrix} m_{1i_s} & \cdots & m_{1i_k} \\ \vdots & \ddots & \vdots \\ m_{s-1i_s} & \cdots & m_{s-1i_k} \end{pmatrix}.$$

From $M'\Delta\delta' = 0$, we get the equation

$$M_I\Delta\delta_I + M_{II}\Delta\delta_{II} = 0(\text{or equivalently } M_I\Delta\delta_I = M_{II}\Delta\delta_{II}).$$

Since M_I is an invertible matrix by lemma 1, we have the equation

$$\Delta\delta_I = M_I^{-1}M_{II}\delta_{II}.$$

Hence $\{\Delta\delta_{i_1} \cdots, \Delta\delta_{i_{s-1}}\}$ are determined by $\{\Delta\delta_{i_s} \cdots, \Delta\delta_{i_k}\}$ ■

Lemma 2 means that the summation in (4) is not taken for all $\Delta\delta_{i_1}, \cdots, \Delta\delta_{i_k}$ but taken for all $\Delta\delta_{j_1}, \cdots, \Delta\delta_{j_{k-s+1}}$ for some index set $\{j_1, \cdots j_{k-s+1}\} \subset \{i_1, \cdots, i_k\}$. Now, we are ready to prove our main theorem.

Theorem 1. *Assume that the round keys, which are xored to the input data at each round, are independent and uniformly random. If $n_d = n+1$, the probability of each differential of SDS function is bounded by p^n.*

Proof Consider the differential as depicted in Fig.3. Let $Hw(\Delta\alpha) = k$ and $Hw(\Delta\beta) = n - s + 1$ $(s \leq k)$, then without loss of generality we may assume

$$\Delta\alpha_1 \neq 0, \cdots, \Delta\alpha_k \neq 0 \tag{5}$$

(equivalently, $\Delta\delta_1 \neq 0, \cdots, \Delta\delta_k \neq 0$) and

$$\Delta\beta_{j_1} \neq 0, \cdots, \Delta\beta_{j_{n-s+1}} \neq 0. \tag{6}$$

(equivalently, $\Delta\gamma_{j_1} \neq 0, \cdots, \Delta\gamma_{j_{n-s+1}} \neq 0$). Then,

$$\begin{aligned} & DP(\Delta\alpha \to \Delta\beta) \\ &= \sum_{\Delta\delta_1, \cdots, \Delta\delta_n} \left(\prod_{i=1}^{n} DP^{S_i}(\Delta\alpha_i \to \Delta\delta_i) \prod_{i=1}^{n} DP^{S_i}(\Delta\gamma_i \to \Delta\beta_i | \Delta\alpha) \right) \\ &= \sum_{\Delta\delta_1, \cdots, \Delta\delta_n} \left(\prod_{i=1}^{n} DP^{S_i}(\Delta\alpha_i \to \Delta\delta_i) \prod_{i=1}^{n} DP^{S_i}(\Delta\gamma_i \to \Delta\beta_i) \right) \qquad (7) \\ &= \sum_{\Delta\delta_1, \cdots, \Delta\delta_k} \left(\prod_{i=1}^{k} DP^{S_i}(\Delta\alpha_i \to \Delta\delta_i) \prod_{i=1}^{n-s+1} DP^{S_{j_i}}(\Delta\gamma_{j_i} \to \Delta\beta_{j_i}) \right) \qquad (8) \end{aligned}$$

$$= \sum_{\Delta\delta_{i_1}\neq 0,\cdots,\Delta\delta_{i_{k-s+1}}\neq 0} \left(\prod_{i=1}^{k} DP^{S_i}(\Delta\alpha_i \to \Delta\delta_i) \prod_{i=1}^{n-s+1} DP^{S_{j_i}}(\Delta\gamma_{j_i} \to \Delta\beta_{j_i}) \right) \quad (9)$$

$$\leq \sum_{\Delta\delta_{i_1}\neq 0,\cdots,\Delta\delta_{i_{k-s+1}}\neq 0} \left(\prod_{t=1}^{k-s+1} DP^{S_{i_t}}(\Delta\alpha_{i_t} \to \Delta\delta_{i_t}) p^{s-1} p^{n-s+1} \right) \quad (10)$$

$$= p^n \sum_{\Delta\delta_{i_1}\neq 0,\cdots,\Delta\delta_{i_{k-s+1}}\neq 0} \left(\prod_{t=1}^{k-s+1} DP^{S_{i_t}}(\Delta\alpha_{i_t} \to \Delta\delta_{i_t}) \right)$$

$$\leq p^n$$

Equation (7) follows from the assumption on round keys; equation (8) follows from assumptions (5) and (6); equation (9) follows from lemma 2; and equation (10) follows from the definition of p. ■

This theorem gives a provable security for the SPN structure.

For example, consider a 128-bit SPN structure with 16 substitution boxes, $S_1, \cdots S_{16}$, and a maximal diffusion layer. If we let

$$\begin{array}{rccc} S_i & : & GF(2^8) \to GF(2^8) \ (1 \leq i \leq n) \\ & & x \quad \to \quad x^{-1} \end{array}$$

we can take $p = 2^{-6}$, so that the maximum differential probability of this SDS function is bounded by $p^{16} = (2^{-6})^{16} = 2^{-96}$. Hence one gets a SPN structure which gives proven resistance of order 2^{-96} against DC.

4 Provable Security against LC

In this section we will give a provable security for the SPN structure with a maximal diffusion layer against LC. We know that the rank of M equals that of M^t for any matrix M and so applying lemma 1 and 2 gives the following result; If $n_d(D)$ is equal to $n+1$, $n_l(D)$ is also $n+1$ and vice versa. Therefore we have the following theorem.

Theorem 2. *If $n_l(D) = n+1$(or equivalently $n_d(D) = n+1$), the probability of each linear hull of SDS function is bounded by q^n.*

5 Provable Security against DC and LC with a Semi-maximal Diffusion Layer

In this section we will show that the probability of each differential is bounded by p^{n-1} when $n_d(D)$ is equal to n. A diffusion layer is called semi-maximal with respect to DC(resp. LC) when $n_d(D)$(resp. $n_l(D)$) equals n. In general $n_d(D)$ is not equal to $n_l(D)$ but there are sufficient conditions that $n_l(D)$ is equal to $n_d(D)$[14]. A diffusion layer is called **semi − maximal** if $n_d(D)$ and $n_l(D)$ are equal to n.

Lemma 3. *If $n_d(D) = n$, the rank of each $k \times k$ submatrix of M is greater than or equal to $k-1$ for all $1 \leq k \leq n$ and there exists at least one $s \times s$ submatrix with rank $s-1$ for some $1 \leq s \leq n$.*

Proof Let $n_d(D) = n$ and suppose that there exists a $k \times k$ submatrix M_k of M whose rank is less than $k-1$. That is, there exist at least two independent vectors $v, w \in GF(2^m)^k$ so that $M_k v = M_k w = 0$. We can make a vector $x \in GF(2^m)^k$ with $Hw(x) \leq k-1$ and $M_k x = 0$ by a linear combination of v and w over $GF(2^m)$. From x and M_k we can get a vector $X \in GF(2^m)^n$ such that $Hw(X) \leq k-1$ and $Hw(MX) \leq n-k$. This is contradiction to the fact that $n_d(D)$ is equal to n. Hence the rank of each $k \times k$ submatrix of M is greater than or equal to $k-1$ for all $1 \leq k \leq n$. By lemma 1 there exists at least one $s \times s$ submatrix with rank $s-1$. ■

We also state a statement similar to lemma 2; Let M be the $n \times n$ matrix representing a diffusion layer D and $n_d(D) = n$. In Fig.3, if $Hw(\Delta\alpha) = k$ and $Hw(\Delta\beta) = n - s(s \leq k)$, there is a index set $\{i_i, \cdots, i_{s-1}\}$ so that $\{\Delta\delta_{i_1}, \cdots, \Delta\delta_{i_{s-1}}\}$ are represented by the other $\Delta\delta_i$'s. The proof of this statement is similar to that of the lemma 2.

Theorem 3. *Assume that the round keys, which are xored to the input data at each round, are independent and uniformly random. If $n_d = n$, the probability of each differential of SDS function is bounded by p^{n-1}.*

Proof We use the same notations as used in the proof of theorem 1. There is only one difference between the proof of theorem 3 and that of this theorem; $Hw(\Delta\beta)$ is not $n-s+1$ but $n-s$. Thus $DP(\Delta\alpha \rightarrow \Delta\beta)$ goes up by p^{-1}. Hence we have

$$DP(\Delta\alpha \rightarrow \Delta\beta) \leq p^{n-1} \quad \blacksquare$$

We can easily check that if $n_l(D) = n$, the probability of linear hull of SDS function is bounded by q^{n-1}.

6 Conclusion

In the SPN structure, it is very important to design a diffusion layer with good properties as well as a substitution layer. Even though a substitution layer is strong against DC and LC, this does not guarantee a secure SPN structure against DC and LC if a diffusion layer does not provide an avalanche effect, both in the context of differences and linear approximations.

In this paper we give the necessary and sufficient condition for diffusion layer to be maximal or semi-maximal. Also we proved that the probability of each differential(resp. linear hull) of the SDS function with a maximal diffusion layer is bounded by p^n(resp. q^n) and that of each differential(resp. linear hull) of the SDS function with a semi-maximal diffusion layer is bounded by p^{n-1}(resp. q^{n-1}). These results give a provable security for the SPN structure against DC and LC with a maximal diffusion layer or a semi-maximal diffusion layer. Therefore we

expect to obtain a SPN structure with a higher resistance against DC and LC and a smaller number of rounds.

References

1. E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystem*, Journal of Cryptoloy, Vol.4, pp. 3-72, 1991.
2. E. Biham and A. Shamir, *Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer*, Advanced in cryptology-CRYPTO'91, pp. 156-171, Springer-Verlag, 1991.
3. E. Biham, *On Matsui's Linear Cryptanalysis*, Advanced in cryptology-EUROCRYPT'94, pp. 341-355, Springer-Verlag, 1994.
4. J. Daemen, R. Govaerts and J. Vandewalle, *Correlation Matrices*, Proceedings of the first international workshop of the Fast Software Encryption, LNCS 1008, pp. 275-285, Springer-Verlag, 1994.
5. M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki and K. Ohta, *A Strategy for Constructing Fast Functions with Practical Security against Differential and Linear Cryptanalysis*, Proceedings of SAC'98, 1998.
6. M. Matsui, *Linear cryptanalysis method for DES cipher*, Advanced in cryptology-EUROCRYPT' 93, pp. 386-397, Springer-Verlag, 1993.
7. M. Matsui, *The first Experimental cryptanalysis of DES*, Advanced in cryptology-CRYPTO'94, pp. 1-11, Springer-Verlag, 1994.
8. M. Matsui, *New Block Encryption Algorithm MISTY*, Proceedings of the fourth international workshop of Fast Software Encryption, Springer-Verlag, pp. 53-67, 1997.
9. K. Nyberg and L. R. Knudsen, *Provable security against a differential attack*, Advanced in cryptology-CRYPTO'92, pp. 566-574, Springer-Verlag, 1992.
10. K. Nyberg, *Differentially uniform mappings for cryptography*, Advanced in cryptology-EUROCRYPT'93, pp. 55-64, Springer-Verlag, 1993.
11. K. Nyberg, *Linear Approximation of block ciphers*, Advanced in cryptology-EUROCRYPT'94, pp. 439-444, Springer-Verlag, 1994.
12. V. Rijmen, J.Daemen et al, *The cipher SHARK*, Proceedings of the fourth international workshop of Fast Software Encryption, pp. 137-151, Springer-Verlag, 1997.
13. J. Daemen and V. Rijmen, *The Rijdael block cipher*, AES proposal, 1998.
14. J. Kang, C. Park, S. Lee and J. Lim, *On the optimal diffusion layer with practical security against Differential and Linear Cryptanalysis*, Preproceedings of ICISC'99, pp. 13-20, 1999.
15. X. Lai, J. L. Massey and S. Murphy *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology-EUROCRYPT'91, pp 17-38, Springer-Verlag, 1992.
16. J. Daemen, *Cipher and hash function design strategies based on linear and differential cryptanalysis,* Doctoral Dissertation, March 1995, K.U. Leuven.
17. K. Aoki and K. Ohta, *Strict Evaluation of the Maximum Average of Differential Probability and the Maximum Average of Linear Probability*, IEICE Transactions Fundamentals of Electronics, Communications and Computer Science, Vol. E80A, No. 1, pp. 2-8, 1997.