Practical and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks

Ju-Sung Kang, Seokhie Hong, Sangjin Lee, Okyeon Yi, Choonsik Park, and Jongin Lim

We examine the diffusion layers of some block ciphers referred to as substitution-permutation networks. We investigate the practical and provable security of these diffusion layers against differential and linear cryptanalysis. First, in terms of practical security, we show that the minimum number of differentially active S-boxes and that of linearly active S-boxes are generally not identical and propose some special conditions in which those are identical. We also study the optimal diffusion effect for some diffusion layers according to their constraints. Second, we obtain the results that the consecutive two rounds of SPN structure provide provable security against differential and linear cryptanalysis, i.e., we prove that the probability of each differential (resp. linear hull) of the consecutive two rounds of SPN structure 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}), where p and q are maximum differential and linear probabilities of the substitution layer, respectively.

Manuscript received May 4, 2001; revised Aug. 17, 2001 and Oct. 9, 2001.

Ju-Sung Kang (phone: +82 42 860 5326, e-mail: jskang@etri.re.kr) is with Information Security Research Division, ETRI, Daejeon, Korea.

Seokhie Hong (e-mail: hsh@cist.korea.ac.kr), Sangjin Lee (e-mail: sanjin@tiger.korea.ac.kr), and Jongin Lim (e-mail: jilim@tiger.korea.ac.kr) are with Center for Information Security Technologies, Korea University, Seoul, Korea.

Okyeon Yi (e-mail: oyyi@kmu.kookmin.ac.kr) is with the Department of Mathematics, Kookmin University, Seoul, Korea.

Choonsik Park (e-mail: csp@etri.re.kr) is with National Security Research Institute, ETRI, Daejeon, Korea.

I. INTRODUCTION

1. Introduction to SPN Structure and Diffusion Layer

Shannon suggested that practical and secure product ciphers maybe constructed by using a mixing transformation consisting of a number of layers or rounds of "confusion" and "diffusion" [1]. The confusion component is a nonlinear substitution on a small subblock and the diffusion component is a linear mixing of the subblock connections. The Substitution-Permutation Networks (SPN) structure is directly based on the concepts of confusion and diffusion. One round of an SPN structure generally consists of three layers of substitution, permutation, and key addition. A substitution layer is made up of small nonlinear substitutions referred to as S-boxes easily implemented by table lookup for confusion effect. A permutation layer is a linear transformation that diffuses the cryptographic characteristics of the substitution layer. A key addition layer implants round subkeys of the cipher and the position of this layer is variable according to ciphers.

Due to memory requirements, most block cipher designers use small S-boxes, e.g. with 4 or 8 input bits. Thus, the diffusion of S-box outputs by a permutation layer plays a great role in providing resistance to various attacks including differential and linear cryptanalysis. On the other hand, permutation layers of most modern block ciphers are not simple bit-wise position permutations or transpositions but linear transformations on some vector spaces over various finite fields. Hence in this paper, we refer to a permutation layer as a "diffusion layer" for the sake of clarity. Most diffusion layers have appropriate matrix representations, since they are linear transformations over

some finite fields and have one-to-one correspondence to an appropriate matrix. With these matrix representations, we study the practical and provable security against differential and linear cryptanalysis.

2. Related Works and Our Results

The most well known method of analyzing block ciphers today is the differential cryptanalysis (DC), proposed by Biham and Shamir [2], [3] in 1990. DC is a chosen plaintext attack in which the attacker chooses some plaintexts of certain well-considered differences. Biham and Shamir used the notion of "characteristic", while Lai, Massey and Murphy [4] showed that the notion "differential" strictly reflects the strength of a cipher against DC. Roughly speaking, a differential is a collection of characteristics.

Another method of analyzing block ciphers is the linear cryptanalysis (LC) published by Matsui [5] in 1993. The attacks based on LC are known plaintext attacks and the attack on the DES is faster than the attack by DC. The first version of LC applied "linear approximation" to an attack of block ciphers, but Nyberg [6] has considered a collection of linear approximation, which she called a "linear hull" for strict evaluation of the strength against LC.

Kanda et al. [7] classified four measures to evaluate the security of a cipher against DC and LC as follows:

- Precise measure: The maximum average of differential and linear hull probabilities [4], [6].
- Theoretical measure: The upper bounds of the maximum average of differential and linear hull probabilities [8]-[11].
- Heuristic measure: The maximum average of differential characteristic and linear approximation probabilities [2], [3], [5].
- Practical measure: The upper bounds of the maximum average of differential characteristic and linear approximation probabilities [12]-[14].

DC and LC are the most powerful attacks to most symmetric block ciphers. Accordingly, it is a basic requisite for the designer to evaluate the security of any new proposed cipher against DC and LC, and to prove that it is sufficiently resistant against them.

In this paper, we consider a practical measure and theoretical measure out of the above four measures. Nyberg and Knudsen [11] stated that Feistel ciphers evaluated with the theoretical measure are provably secure against DC and LC. Therefore, a block cipher is called to have *provable security* against DC and LC, where the upper bounds of the maximum average of differential and linear hull probabilities are sufficiently small. Meanwhile, Knudsen [13] noted that Feistel ciphers evaluated with the practical measure are practically secure against DC and LC. Thus, a block cipher is called to have *practical security* against DC and LC if the upper bounds of the maximum average of differential characteristic and linear approximation probabilities are sufficiently small.

First, we show that in terms of practical security, the minimum number of differentially active S-boxes and that of linearly active S-boxes are generally not identical and propose some special conditions in which those are identical. We also show that all diffusion layers of E2, Crypton and Rijndael have achieved optimal diffusion effects according to their each constraint of using operations. Second, the consecutive two rounds of SPN structure are shown to provide provable security against differential and linear cryptanalysis, where the diffusion layer has a maximal or semi-maximal diffusion effect, i.e., we prove that the probability of each differential (resp. linear hull) of the consecutive two rounds of SPN structure 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}), where p and q are maximum differential and linear probabilities of the substitution layer, respectively. This paper is the refined version of [15] and [16].

II. PRELIMINARIES

1. Basic Definitions

Let S be an S-box with m input and output bits, i.e., $S : Z_2^m \rightarrow Z_2^m$. Differential and linear probabilities of S are defined as the following definition.

Definition 1 For any given Δx, Δy; Γx; $\Gamma y \in Z_2^m$, define differential and linear probabilities of S by

$$DP^S(\Delta x \rightarrow \Delta y) = (1/2^m)\,(\#\{x \in Z_2^m : S(x) \oplus S(x \oplus \Delta x) = \Delta y\})$$

and

$$LP^S(\Gamma y \rightarrow \Gamma x) = [\,(1/2^{m-1})\,(\#\{x \in Z_2^m : \Gamma x \bullet x = \Gamma y \bullet S(x)\}) - 1\,]^2,$$

respectively, where $a \bullet b$ denotes the parity (0 or 1) of bit-wise product of a and b.

DP^S and LP^S for a strong S-box S should be small enough for any input difference $\Delta x \neq 0$ and output mask value $\Gamma y \neq 0$. Therefore, we define parameters that represent resistance to DC and LC of an S-box and each substitution layer of an SPN structure as the following definition.

Definition 2 The maximum differential and linear probabilities of S are defined by

$$DP^S_{\max} = \max_{\Delta x \neq 0, \Delta y} DP^S(\Delta x \rightarrow \Delta y)$$

and

$$LP^S_{\max} = \max_{\Gamma x, \Gamma y \neq 0} LP^S(\Gamma y \rightarrow \Gamma x),$$

respectively.

2. Differentially and Linearly Active S-Boxes

Evaluation of security for a block cipher of SPN structure by a practical measure begins with the concept of an active S-box. The following five definitions and one theorem of this subsection are already written in some previous works [7], [14], [16], [17]. At this point, we slightly revise some definitions in order to describe our results.

Definition 3 A *differentially active S-box* is defined as an S-box given a non-zero input difference and a *linearly active S-box* as an S-box given a nonzero output mask value.

By computing the minimum number of differentially and linearly active S-boxes, we can evaluate security of a block cipher in terms of practical security against DC and LC [12]-[14], [17]. We can obtain upper bounds of the maximum differential characteristic and linear approximation probabilities from the minimum number of active S-boxes. Thus, in the case of an SPN structure, it is important to analyze the increasing amounts of minimum number of active S-boxes by considering a diffusion layer in consecutive two rounds.

Note that we can omit the key addition layer to compute the number of active S-boxes since this layer has no influence under the assumption that the key addition layer is performed by bit-wise EXORs. Define the SDS function with three layers of substitution-diffusion-substitution for analyzing the role of a diffusion layer to increase the number of active S-boxes in consecutive two rounds of an SPN structure (Fig. 1).

Throughout this paper, we consider the SDS function with mn-bit input and output values and assume that all S-boxes in the substitution layer are $m \times m$ and bijective. If an S-box is bijective and differentially/linearly active, then it has a non-zero output difference/input mask value [10]. Therefore, when all S-boxes in substitution layer are bijective, we can define the minimum number of active S-boxes of the SDS function. Denote the diffusion layer of SDS function as D, input difference of D as $\Delta x = x \oplus x^*$, output difference as $\Delta y = y \oplus y^* = D(x) \oplus D(x^*)$, and input and output mask value as Γx and Γy, respectively.

Definition 4 The minimum number of differentially and linearly active S-boxes of the SDS function are defined by

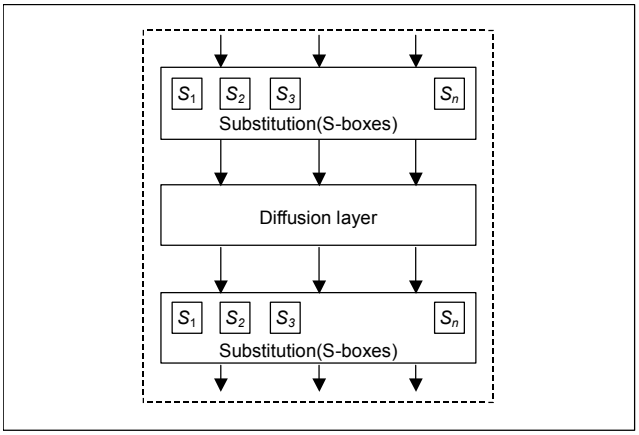


Fig. 1. SDS function.

$$\beta_d(D) = \min_{\Delta x \neq 0} \{ H_c(\Delta x) + H_c(\Delta y) \}$$

and

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

respectively, where, for each $x = (x_1, x_2, \ldots, x_n) \in (Z_2^m)^n$ or $GF(2^m)^n$, the component Hamming weight of x is defined by $H_c(x) = \#\{ 1 \le i \le n : x_i \neq 0 \}$.

$\beta_d(D)$ and $\beta_l(D)$ are lower bounds for the number of active S-boxes in two consecutive rounds of a differential characteristic and linear approximation, respectively. On the other hand, from the minimality, we can see that $\beta_d(D)$ and $\beta_l(D)$ are at most n+1 by considering $H_c(\Delta x) = H_c(\Gamma y) = 1$. So a diffusion layer is called *maximal* if the $\beta_d(D)$ and $\beta_l(D)$ are n+1.

Now we can define differential characteristic and linear approximation probabilities of the SDS function like the definitions for S-boxes. See Figs. 2 and 3.

Definition 5 For any given Δx, Δy, Γx, $\Gamma y \in Z_2^{mn}$, define the differential characteristic and linear approximation probabilities of the SDS function by

$$DCP^{SDS}(\Delta x \rightarrow \Delta y)$$
$$= \max_{\Delta w} \prod_{i=1}^{n} DP^{S_i}(\Delta x_i \rightarrow \Delta w_i) \cdot DP^{S_i}(D(\Delta w_i) \rightarrow \Delta y_i)$$

and

$$LAP^{SDS}(\Gamma y \rightarrow \Gamma x)$$
$$= \max_{\Gamma z} \prod_{i=1}^{n} LP^{S_i}(\Gamma y_i \rightarrow \Gamma z_i) \cdot LP^{S_i}(D^{-1}(\Gamma z)_i \rightarrow \Gamma x_i),$$

respectively, where $\Delta x = (\Delta x_1, \ldots, \Delta x_n) \in (Z_2^m)^n$ and Δy, Δw, Γx, Γy, Γz are denoted in the same way as Δx.. Here, $D(\Delta w) = (D(\Delta w)_1, \ldots, D(\Delta w)_n)$ and $D^{-1}(\Gamma z) = (D^{-1}(\Gamma z)_1, \ldots, D^{-1}(\Gamma z)_n)$ denote the output difference and input mask value of the diffusion layer D with probability 1, respectively.

Definition 6 The maximum differential characteristic and lin-

ear approximation probabilities of the SDS function are defined by

$$DCP^{SDS}{}_{\max} = \max_{\Delta x \neq 0, \Delta y} DCP^{SDS}(\Delta x \to \Delta y)$$

and

$$LAP^{SDS}{}_{\max} = \max_{\Gamma x, \Gamma y \neq 0} LAP^{SDS}(\Gamma y \to \Gamma x),$$

respectively.

Definition 7 Assume that the substitution layer of an SDS function consists of n S-boxes $S_1, S_2, \ldots, S_n$. The maximum differential and linear probabilities of the substitution layer are defined by

$$p = \max_{1 \le i \le n} DP^{Si}{}_{\max} \quad \text{and} \quad q = \max_{1 \le i \le n} LP^{Si}{}_{\max},$$

respectively.

Theorem 1 The maximum differential characteristic and linear approximation probabilities $DCP^{SDS}{}_{\max}$ and $LAP^{SDS}{}_{\max}$ of the SDS function hold for

$$DCP^{SDS}{}_{\max} \le p^{\beta_d(D)} \quad \text{and} \quad LAP^{SDS}{}_{\max} \le q^{\beta_l(D)}.$$

The above theorem is obtained easily by the maximality of p(or q) and the minimality of $\beta_d(D)$ (or $\beta_l(D)$). Evaluation of practical security against DC and LC is based on this theorem.

III. PRACTICAL SECURITY AGAINST DC AND LC

1. Matrix Representation of a Diffusion Layer

Most diffusion layers of modern block ciphers of an SPN structure are linear transformations on the vector space $GF(2^m)^n$ and have one-to-one correspondence to an appropriate matrix. That is, most diffusion layers have appropriate matrix representations. If we use this matrix representation for a diffusion layer, then we obtain the relationship between input and output differences (or mask values). 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 $m_{ij} \in GF(2^m)$. Hence we only need to investigate the matrix M to analyze the role of the diffusion layer D.

To begin, we describe some notations and definitions. Without loss of generality, we may assume

$$GF(2^m) = \{ a_0 + a_1\gamma + a_2\gamma^2 + \ldots + a_{m-1}\gamma^{m-1} \mid a_i \in \{0,1\} \}$$

for some $\gamma \in GF(2^m)$. In general, we can regard the finite field $GF(2^m)$ as the m-dimensional vector space over $GF(2)$ and $GF(2^m)^n$ as the mn-dimensional vector space over $GF(2)$. We will use a notation $\vec{a} \in GF(2)^m$ as the column vector corresponding to $a \in GF(2^m)$ and $\vec{\xi} \in GF(2)^{mn}$ as the column vector corresponding to $\xi \in GF(2^m)^n$.

By assumption of diffusion layer, we can rewrite $\beta_d(D)$ as follows:

$$\beta_d(D) = \min_{\Delta x \neq 0} \{ H_c(\Delta x) + H_c(M\Delta x) \}.$$

Now, we consider $\beta_l(D)$. Let's define a map ϕ from $GF(2^m)$ to $GF(2)$ as follows:

$$\phi(a) = \oplus_{i=0}^{m-1} a_i,$$

where $a = \Sigma_{i=0}^{m-1} a_i \gamma^i$, $a_i \in \{0,1\}$.

Lemma 1 There exists an unique $m \times m$ binary invertible matrix B so that $\phi(a \cdot b) = \vec{a}^{\,t} B \vec{b}$ for all $a, b \in GF(2^m)$, where t suffix denotes transposition of a vector.

Proof: Let $a = \Sigma_{i=0}^{m-1} a_i \gamma^i$ and $b = \Sigma_{i=0}^{m-1} b_i \gamma^i$ be two general elements in $GF(2^m)$ and c be $a \cdot b = \Sigma_{i=0}^{m-1} c_i \gamma^i$. Then $c_k = \oplus_{(i,j) \in I_k} a_i b_j$ for some index set I_k and $\phi(c) = \oplus_{i=0}^{m-1} c_i = \oplus_{(i,j) \in I} a_i b_j$ where $I = \cup_{k=0}^{m-1} I_k$ except its elements need not be distinct. Let n_{ij} be the repetition number of $(i,j) \in I$ and $b_{ij} \equiv n_{ij} \bmod 2$. Consider a matrix B whose ith row and jth column is b_{ij}. By definition of B, $\phi(a \cdot b) = \vec{a}^{\,t} B \vec{b}$. It remains to prove B is invertible. Suppose B is not invertible then there exists a nonzero element $a \in GF(2^m)$ so that $\vec{a}^{\,t} B = 0$. $\phi(a \cdot a^{-1}) = \vec{a}^{\,t} B \vec{a}^{-1} = 0$ but it is a contradiction to the fact $\phi(a \cdot a^{-1}) = \phi(1) = 1$. Hence B is invertible. □

Let $\xi = (\xi_1, \ldots \xi_n)^t$, $\eta = (\eta_1, \ldots \eta_n)^t \in GF(2^m)^n$. A scalar product on $GF(2^m)^n$ over $GF(2^m)$ and over $GF(2)$ are denoted by $<,>_m$ and $<,>$, respectively and defined by:

$$<,>_m : GF(2^m)^n \times GF(2^m)^n \to GF(2^m)$$
$$(\xi, \eta) \mapsto \xi_1 \cdot \eta_1 + \ldots + \xi_n \cdot \eta_n$$
$$<,> : GF(2^m)^n \times GF(2^m)^n \to GF(2)$$
$$(\xi, \eta) \mapsto \vec{\xi}^{\,t} \cdot \vec{\eta}.$$

As a matter of convenience we denote the field element corresponding to $B\vec{a} \in GF(2)^m$ by Ba. Let $\tilde{\eta} = (B\eta_1, \ldots B\eta_n) \in GF(2^m)^n$ and $\hat{\eta} = (B^{-1}\eta_1, \ldots B^{-1}\eta_n) \in GF(2^m)^n$. By definitions of $<,>$, $<,>_m$ and ϕ,

$$\begin{aligned} <\xi, \eta> &= \vec{\xi}_1^{\,t} BB^{-1} \vec{\eta}_1 \oplus \cdots \oplus \vec{\xi}_n^{\,t} BB^{-1} \vec{\eta}_n \\ &= \phi\left(<\xi, \hat{\eta}>_m\right) \\ &= \phi\left(<M^{-1}\xi, M^t\hat{\eta}>_m\right) \\ &= <M^{-1}\xi, \tilde{M^t}\hat{\eta}>. \end{aligned}$$

Hence we obtain the following lemma.

Lemma 2 Let Γy be an output mask value of diffusion layer D then the input mask value becomes $M^{t}\hat{\Gamma}y$.

It is indicated from Lemma 2 that if M is a binary matrix, $\Gamma x = M^t \Gamma y$, and this result is shown in [17].

Corollary 1 The minimum number of linearly active S-boxes is

$$\min_{\Gamma y \neq 0} \{ H_c(M^t \Gamma y) + H_c(\Gamma y) \} .$$

Proof: This corollary follows from Lemma 2 and the fact that there exist one-to-one correspondences between η, $\hat{\eta}$, and $\hat{\eta}$ and $H_c(\eta) = H_c(\hat{\eta}) = H_c(\tilde{\eta})$ for any $\eta \in GF(2^m)^n$. □

It is possible that we compute the minimum numbers of differentially and linearly active S-boxes ($\beta_d(D)$ and $\beta_l(D)$) of the SDS function by using the above matrix representation. However, the minimum numbers of differentially and linearly active S-boxes are not identical in general. In the next subsection, we will show that $\beta_d(D) \neq \beta_l(D)$ by proposing a counterexample. On the other hand, the minimum numbers of differentially and linearly active S-boxes are identical for the special types of representation matrix M as the following two theorems.

Theorem 2 Let the diffusion layer D of the SDS function be represented as $n \times n$ matrix M. If M is a symmetric or orthogonal matrix, then $\beta_d(D) = \beta_l(D)$.

Proof: Observe that

$$\beta_d(D) = \min_{\Delta x \neq 0} \{ H_c(\Delta x) + H_c(M\Delta x) \} ,$$
$$\beta_l(D) = \min_{\Gamma y \neq 0} \{ H_c(M^t \Gamma y) + H_c(\Gamma y) \} .$$

From this, we can easily see that $\beta_d(D) = \beta_l(D)$ if M is a symmetric matrix where $M^t = M$. Meanwhile, if M is an orthogonal matrix that $M^{-1} = M^t$, then $\Gamma x = M^t \Gamma y$ implies that $\Gamma y = M\Gamma x$, and the condition $\Gamma y = M\Gamma x \neq 0$ is identical to $\Gamma x \neq 0$ since M is an invertible matrix. Thus

$$\beta_l(D) = \min_{\Gamma x \neq 0} \{ H_c(\Gamma x) + H_c(M\Gamma x) \} ,$$

so $\beta_d(D) = \beta_l(D)$. □

Theorem 3 If M^t is obtained from M by applying operations of exchanging row or column vectors, then $\beta_d(D) = \beta_l(D)$.

Proof: The operation of exchanging row vectors of M results in changing the order of components of output difference Δy, and this operation does not affect the component Hamming weight $H_c(\Delta y)$. On the other hand, it is clear that $H_c(\Delta y)$ is determined by column vectors of M but not by their location. Thus, the operation of exchanging column vectors of M also does not affect the component Hamming weight $H_c(\Delta y)$. Since a row(column) vector of M is a column(row) vector of M^t, operations of exchanging row or column vectors of M does not affect the component Hamming weight. Therefore, if M^t is obtained from M by those operations, $\beta_d(D) = \beta_l(D)$. □

It is easy to see that the diffusion layer of block cipher CRYPTON [18] is represented as a symmetric matrix. Hence, we obtain $\beta_d(D) = \beta_l(D)$ by Theorem 2, in this case [16]. On the other hand, in [16] authors also showed that for the diffusion layers of block cipher Rijndael [19] and E2 [20], Theorem 3 can be applied.

2. Optimal Diffusion Effects of Diffusion Layers under Some Constraints

Assume that inputs of the SDS function are linearly transformed to outputs per M-bit and the diffusion layer is constructed with just bitwise EXORs. The diffusion layer is represented as an $n \times n$ matrix M where all entries are zero or one as follows:

$$y_i = \oplus_{j=1}^{n} \mu_{ij} x_{ij} = \oplus \mu_{ij=1}^{n} x_{ij} ,$$

where $x = (x_1, x_2, \ldots, x_n) \in (Z_2^m)^n$ is an input, $y = (y_1, y_2, \ldots, y_n)$ is the output, and $M = (\mu_{ij})$.

Kanda et al. [7] studied diffusion properties of the diffusion layer with this matrix representation. Their study was based on the relationship between the matrix for differential characteristic and linear approximation. However, they made two conjectures to unfold their theory. The Conjecture 1 in [7] is correct since this is a special case of Theorem 2, but the Conjecture 2 in [7] is a wrong opinion. We disprove this conjecture by proposing a counterexample.

Conjecture 2 of [7] In the SDS function, the minimum number of differentially active S-boxes is equal to the minimum number of lineally active S-boxes. That is, $\beta_d(D) = \beta_l(D)$, where M is the representation matrix of the diffusion layer D.

Counterexample for the Conjecture 2 of [7]: Suppose that the diffusion layer of SDS function with n=4 be represented by the following invertible matrix:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad M^t = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

If $H_c(\Delta x) = 1$, then $H_c(\Delta y) \geq 2$ since $H_c(\Delta y)$ is determined by a column vector of M and Hamming weight of each column vector is at least 2. $H_c(\Delta y)$ is determined by the EXORs between

any different two column vectors if $H_c(\Delta x) = 2$. Any EXOR between two column vectors has the Hamming weight of at least 1. Thus, the minimum number of differentially active S-boxes is $\beta_d(D) = 3$.

On the other hand, in Lemma 2, the relationship between output and input mask values is represented as the transpose matrix M^t of M. Note that the Hamming weight of the fourth column vector of M^t is 1. Consider the output mask value of the form $b = (0, 0, 0, b_4)$, $b_4 \neq 0$, and

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ b_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ b_4 \\ 0 \end{pmatrix},$$

then corresponding input mask value $a = (0, 0, b_4, 0)$. From this we can obtain $\beta_l(D) = 2$. Consequently we know that $\beta_d(D) \neq \beta_l(D)$ for the above 4×4 matrix M. □

In the block cipher E2, designers considered the SDS function with $n = 8$. Kanda et al. [7] suggested a method of determining an 8×8 matrix M yielding the maximum value of $\beta_d(D)$ using the search algorithm. Using this search algorithm, they found that there is no matrix with $\beta_d(D) \geq 6$, and that there are some candidate matrices with $\beta_d(D) = 5$. Here, we give a theoretical proof for the fact that $\beta_d(D) = 5$ is optimal and also that $\beta_l(D) \leq 5$, where M is an 8×8 binary invertible matrix.

Theorem 4 Assume that the number of S-boxes in the substitution layer of the SDS function is 8(n=8). If the representation matrix M of the diffusion layer is an 8×8 binary invertible matrix, then $\beta_d(D), \beta_l(D) \leq 5$.

Proof: Since M is an 8×8 binary invertible matrix, eight column vectors $M_1, M_2, \ldots, M_8$ are linearly independent. Thus, the number of columns with the Hamming weight 8 is at most one. Note that $\beta_d(D)$ is closely related to the Hamming weights of column vectors of M. We separate the proof into four cases. Here, the Hamming weight $H_c(M_j)$ of a column vector M_j is the number of entries with 1 in M_j.

Case 1 If $\min_{1 \leq j \leq 8} H_c(M_j) = 7$, for any two column vectors M_j and M_k, $H_c(M_j \oplus M_k) \leq 2$. By considering Δx such that $H_c(\Delta x) = 2$, we obtain that $\beta_d(D) \leq 2 + 2 = 4$.

Case 2 Suppose that $\min_{1 \leq j \leq 8} H_c(M_j) = 6$. If there exists a column vector with Hamming weight 8, then $H_c(\Delta y) \leq 2$ for some Δx such that $H_c(\Delta x) = 2$. If there exists a column vector with Hamming weight 7, the minimum value of $H_c(\Delta y)$ is at most 3, since we can consider the EXORs between the columns with Hamming weight 6 and 7, where $H_c(\Delta x) = 2$. Finally, if the Hamming weight of all column vectors is 6, then although some different four column vectors include 0 entries in distinct rows, the Hamming weight of EXORs between one of this four columns and another fifth column vector is 2. Consequently, we obtain that $\beta_d(D) \leq 5$.

Case 3 Assume that $\min_{1 \leq j \leq 8} H_c(M_j) = 6$. If there exists a column vector with the Hamming weight 8, then $H_c(\Delta y) \leq 3$ for some Δx so that $H_c(\Delta x) = 2$. If there exists a column vector with the Hamming weight 7 or 6, by a similar analysis as in *Case 2*, we can obtain what we want. In the case that the Hamming weight of each column vectors is 5, although 0 entries of some different five column vectors are arranged optimally, another sixth column vector and one of these five columns have in common at least two 0 entries at the same rows. Thus, $H_c(\Delta y)$ is at most 2 where $H_c(\Delta x) = 2$. Therefore, $\beta_d(D) \leq 5$ also holds in this case.

Case 4 Assume that $\min_{1 \leq j \leq 8} H_c(M_j) \leq 4$. Consider only Δx such that $H_c(\Delta x) = 1$. Then, we easily obtain $\beta_d(D) \leq 5$ since there exists a column with the Hamming weight 4.

By *Cases 1* to *4*, we obtain that $\beta_d(D) \leq 5$ always holds whenever M is an 8×8 binary invertible matrix. On the other hand, by Theorem 2, $\beta_l(D)$ is related to M^t. Thus, we can also obtain the same result for $\beta_l(D)$ by considering the Hamming weight of row vectors instead of column vectors of M. □

The diffusion layer of block cipher CRYPTON [18] consists of bitwise EXOR and AND logic. In this case, we can also theoretically show that the optimality of the diffusion layer by the similar process of the proof of Theorem 4. On the other hand, in the block cipher Rijndael, the maximal diffusion layer is used. It was shown that the maximality of this diffusion layer was obtained by using a maximal distance separable code [14]. This fact also can be shown by the similar methods used in the proof of Theorem 4. Since the additive operation of the finite field $GF(2^m)$ is the bit-wise EXOR, the Hamming weights of EXORs among column vectors of the matrix are reflected to compute β_d. See [16] for the details.

IV. PROVABLE SECURITY AGAINST DC AND LC FOR THE MAXIMAL DIFFUSION LAYER

In this section we will give a provable security for the SDS function with a maximal diffusion layer against DC and LC. Recall that a diffusion layer is called maximal if $\beta_d(D) = \beta_l(D) = n+1$. By Theorem 1, we know that the practical security for the SDS function with a maximal diffusion layer can be estimated as

$$DCP^{SDS}{}_{\max} \leq p^{n+1} \quad \text{and} \quad LAP^{SDS}{}_{\max} \leq q^{n+1}.$$

However, this does not give provable security on the viewpoint of theoretic measure.

Now we consider the provable security against DC and LC on the point of view of differential and linear hull. Let us call M' an $s \times k$ submatrix of M if M' is of the following form:

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

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

Lemma 3 Let M be the $n \times n$ matrix representing a diffusion layer D. Then $\beta_d(D) = n+1$ if and only if the rank of each $k \times k$ submatrix of M is k for all $1 \le k \le n$.

Proof: This lemma was proven in [21]. □

Corollary 2 If $\beta_d(D)$ is equal to $n+1$, $\beta_l(D)$ is also $n+1$ and vice versa.

Proof: This can be drawn by the fact that the rank of M equals that of M^t for any matrix M. □

In [22], 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

$$D : GF(2^m)^n \to GF(2^m)^n$$
$$x \mapsto Bx$$

is a maximal diffusion layer by Lemma 3.

It is not necessary to fix the values of intermediate differences when we consider differentials of SDS function. Therefore, the differential characteristic of SDS function with input difference Δx and output difference Δy is defined by

$$DP^{SDS}(\Delta x \to \Delta y) = \sum_{\Delta w_1, \ldots, \Delta w_n} \left[\prod_{i=1}^{n} DP^{S_i}(\Delta x_i \to \Delta w_i) \cdot \prod_{i=1}^{n} DP^{S_i}(\Delta z_i \to \Delta y_i) \right], \quad (1)$$

where Δw can have any output difference value in the first substitution layer and Δz is $D(\Delta w)$. By similar argument, we can define linear hull probability with input mask value Γx and output mask value Γy as follows:

$$LP^{SDS}(\Gamma y \to \Gamma x) = \sum_{\Gamma z_1, \ldots, \Gamma z_n} \left[\prod_{i=1}^{n} LP^{S_i}(\Gamma y_i \to \Gamma z_i) \cdot \prod_{i=1}^{n} LP^{S_i}(\Gamma w_i \to \Gamma x_i) \right],$$

where Γz is every possible input mask value of second substitution layer and $\Gamma w = D^{-1}(\Gamma z)$.

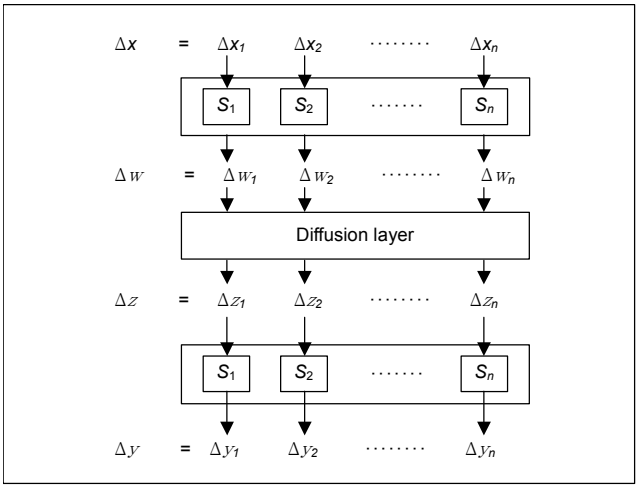


Fig. 2. Differential of SDS function.

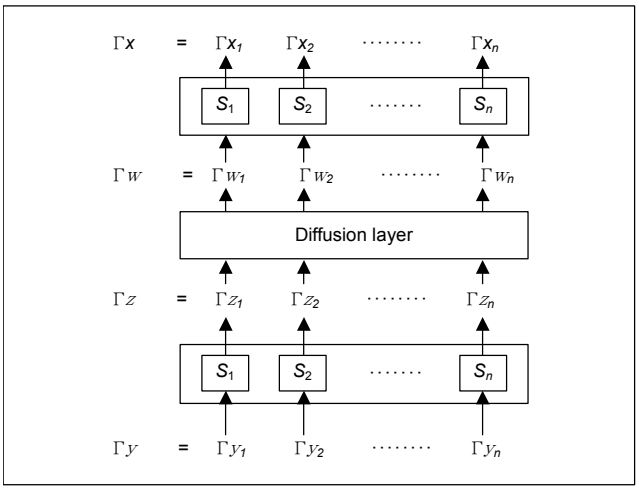


Fig. 3. Linear hull of SDS function.

Definition 8 The maximum differential and linear hull probabilities of the SDS function are defined by

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

and

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

respectively.

Lemma 4 Let M be the $n \times n$ matrix representing a diffusion layer D and $\beta_d(D) = n+1$. In Fig. 2, if $H_c(\Delta x) = k$ and $H_c(\Delta y) = n-s+1$ ($s \le k$), then there is an index set $\{ i_1, \ldots, i_{s-1} \}$ such that $\Delta x_{i_1} \neq 0, \ldots, \Delta x_{i_{s-1}} \neq 0$ and $\{\Delta w_{i_1}, \ldots, \Delta w_{i_{s-1}}\}$ are determined by the other Δw_i's.

Proof: Without loss of generality we may assume $\Delta y_1 = 0, \ldots, \Delta y_{s-1} = 0$ (or equivalently $\Delta z_1 = 0, \ldots, \Delta z_{s-1} = 0$).

Let $\Delta w' = (\Delta w_{i_1}, \ldots, \Delta w_{i_k})^t$ be the collection of all non-zero components in $\Delta w' = (\Delta w_1, \ldots, \Delta w_n)^t$. That is, $\Delta w_{i_j} \neq 0$ for all $1 \leq j \leq k$ and $\Delta w_n = 0$ if $t \notin \{i_1, \ldots, i_k\}$. 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 $\Delta w'$ and the assumption on Δy, $M'\Delta w' = 0$. Let us divide $\Delta w'$ into two parts, Δw_{I} and Δw_{II}, and M' into M_{I} and M_{II} as followings:

$$\Delta w_{\mathrm{I}} = (\Delta w_{i_1}, \ldots, \Delta w_{i_{s-1}})^t,$$
$$\Delta w_{\mathrm{II}} = (\Delta w_{i_s}, \ldots, \Delta w_{i_k})^t,$$

$$M_I = \begin{pmatrix} m_{1i_1} & \cdots & m_{1i_{s-1}} \\ \vdots & \ddots & \vdots \\ m_{s-1i_1} & \cdots & m_{s-1i_{s-1}} \end{pmatrix}$$

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 $M'\Delta w' = 0$, we get $M_{\mathrm{I}}\Delta w_{\mathrm{I}} + M_{\mathrm{II}}\Delta w_{\mathrm{II}} = 0$ (or equivalently $M_{\mathrm{I}}\Delta w_{\mathrm{I}} = -M_{\mathrm{II}}\Delta w_{\mathrm{II}}$). Since M_{I} is an invertible matrix by Lemma 3, we have the equation:

$$\Delta w_{\mathrm{I}} = -M_{\mathrm{I}}^{-1} M_{\mathrm{II}} \Delta w_{\mathrm{II}}.$$

Hence $\{\Delta w_{i_1}, \ldots, \Delta w_{i_{s-1}}\}$ are determined by $\{\Delta w_{i_s}, \ldots, \Delta w_{i_k}\}$. □

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

Theorem 5 If $\beta_d(D) = n+1$, $DP^{SDS}{}_{\max}$ of the SDS function is bounded by p^n.

Proof: Consider the differential as depicted in Fig. 2. Let $H_c(\Delta x) = k$ and $H_c(\Delta y) = n\text{-}s+1$ ($s \leq k$), then without loss of generality we may assume

$$\Delta x_1 \neq 0, \ldots, \Delta x_k \neq 0 \quad (2)$$

(equivalently, $\Delta w_1 \neq 0, \ldots, \Delta w_k \neq 0$) and

$$\Delta y_{j_1} \neq 0, \ldots, \Delta y_{j_{n-s+1}} \neq 0 \quad (3)$$

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

$$DP^{SDS}(\Delta x \to \Delta y)$$
$$= \sum_{\Delta w_1, \ldots, \Delta w_n} \left[\prod_{i=1}^{n} DP^{S_i}(\Delta x_i \to \Delta w_i) \cdot \prod_{i=1}^{n} DP^{S_i}(\Delta z_i \to \Delta y_i)\right]$$
$$= \sum_{\Delta w_1, \ldots, \Delta w_k} \Big[\prod_{i=1}^{k} DP^{S_i}(\Delta x_i \to \Delta w_i) \times \prod_{i=1}^{n-s+1} DP^{S_{j_i}}(\Delta z_{j_i} \to \Delta y_{j_i})\Big] \quad (4)$$
$$= \sum_{\Delta w_{i_1} \neq 0, \ldots, \Delta w_{i_{k-s+1}} \neq 0} \Big[\prod_{i=1}^{k} DP^{S_i}(\Delta x_i \to \Delta w_i) \times \prod_{l=1}^{n-s+1} DP^{S_{j_i}}(\Delta z_{j_i} \to \Delta y_{j_i})\Big] \quad (5)$$
$$\leq \sum_{\Delta w_{i_1} \neq 0, \ldots, \Delta w_{i_{k-s+1}} \neq 0} \left[\prod_{l=1}^{k-s+1} DP^{S_{i_l}}(\Delta x_{i_t} \to \Delta w_{i_t}) \cdot p^{s-1} p^{n-s+1}\right]$$
$$= p^n \sum_{\Delta w_{i_1} \neq 0, \ldots, \Delta w_{i_{k-s+1}} \neq 0} \left[\prod_{l=1}^{k-s+1} DP^{S_{i_l}}(\Delta x_{i_t} \to \Delta w_{i_t})\right] \leq p \quad (6)$$

Equation (4) follows from assumptions (2) and (3), (5) follows from Lemma 4, and the inequality (6) follows from the definition of p. □

We apply similar argument to LC. Therefore, we can conclude the following theorem.

Theorem 6 If $\beta_l(D) = n+1$, $LP^{SDS}{}_{\max}$ of the SDS function is bounded by q^n.

Proof: A proof of this theorem is very similar to that of Theorem 5. □

V. PROVABLE SECURITY AGAINST DC AND LC FOR THE SEMI-MAXIMAL DIFFUSION LAYER

In this section, we show that the probability of each differential (resp. linear hull) is bounded by p^{n-1} (resp. q^{n-1}) when $\beta_d(D)$ (resp. $\beta_l(D)$) is equal to n. A diffusion layer is called semi-maximal with respect to DC (resp. LC) when $\beta_d(D)$ (resp. $\beta_l(D)$) equals n. Also we say that a diffusion layer is *semi-maximal* if $\beta_d(D)$ and $\beta_l(D)$ are equal to n.

Lemma 5 If $\beta_d(D) = n$, then 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 submatix with rank s-1 for some $1 \leq s \leq n$.

Proof: Let $\beta_d(D) = n$ 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 $H_c(x) \leq k$-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 $H_c(X) \leq k$-1 and $H_c(MX) \leq n$-k. This contradicts to the fact that $\beta_d(D)$ 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 $1 \le k \le n$. By Lemma 3, there exists at least one $s \times$ s submatrix with rank s-1. □

We also give a statement similar to Lemma 4. Let M be the $n \times n$ matrix representing a diffusion layer D and $\beta_d(D) = n$. In Fig. 2, if $H_c(\Delta x) = k$ and $H_c(\Delta y) = n$-s ($s \le k$), there is an index set $\{i_1, \ldots, i_{s-1}\}$ such that $\{\Delta w_{i_1}, \ldots, \Delta w_{i_{s-1}}\}$ are represented by the other Δw_i's. A proof of this statement is similar to that of Lemma 4.

Theorem 7 If $\beta_d(D) = n$, $DP^{SDS}_{\max}$ of the SDS function is bounded by p^{n-1}.

Proof: We use the same notations as used in the proof of Theorem 5. There is only one difference between the proof of Theorem 5 and that of this theorem; $H_c(\Delta y)$ is not n-s+1 but n-s. Thus DP^{SDS} ($\Delta x \rightarrow \Delta y$) goes up by p^{-1}. Hence we have $DP^{SDS}_{\max} \le p^{n-1}$. □

Corollary 3 If $\beta_l(D) = n$, $LP^{SDS}_{\max}$ of the SDS function is bounded by q^{n-1}.

We can generalize Theorem 7 and Corollary 3 and get the following theorem.

Theorem 8 If $\beta_d(D) = n$-t (or $\beta_l(D) = n$-t), $DP^{SDS}_{\max}$ (or $LP^{SDS}_{\max}$) of the SDS function is bounded by $p^{n-(t+1)}$ (or $q^{n-(t+1)}$).

Sketch of Proof: Note that an $u \times v$ matrix with a rank w contains a $w \times w$ invertible submatrix. It can be easily checked that if $\beta_d(D) = n$-t, then the rank of each $k \times k$ submatrix of M is greater than or equal to k-t-1 for all t+1 $\le k \le n$. In Fig. 2, let $H_c(\Delta x) = k$ and $H_c(\Delta y) = n$-s ($s \le k$). Then, we can prove there is an index set $\{i_1, \ldots, i_{s-1}\}$ such that $\{\Delta w_{i_1}, \ldots, \Delta w_{i_{s-1}}\}$ are represented by the other Δw_i's. By similar argument to the proof of Theorem 7, it can be shown that $DP^{SDS}_{\max} \le p^{n-(t+1)}$. □

VI. CONCLUSION

We examined the diffusion layers of some block ciphers referred to as substitution-permutation networks. We investigated the practical security of diffusion layers against differential and linear cryptanalysis by using the notion of active S-boxes. We showed that the minimum number of differentially active S-boxes and that of linearly active S-boxes were generally not identical and proposed some special conditions in which those were identical. The optimal diffusion effects for some diffusion layers according to their each constraint were also studied. In terms of provable security, we proved that the probability of each differential (resp. linear hull) of the SDS function with a maximal diffusion layer was 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 was bounded by p^{n-1} (resp. q^{n-1}), where p and q were maximum differential and linear probabilities of the substitution layer, respectively.

REFERENCES

[1] C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Tech. J.*, 28, 1949, pp. 656-715.

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-Like Cryptosystems," *Advances in Cryptology-CRYPTO'90*, LNCS 537, Springer-Verlag, 1990, pp. 2-21.

[3] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-Like Cryptosystems," *J. of Cryptology*, no. 4, 1991, pp. 3-72.

[4] X. Lai, J.L. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," *Advances in Cryptology-Eurocrypt'91*, LNCS 547, Springer-Verlag, 1991, pp. 17-38.

[5] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," *Advances in Cryptology-Eurocrypt'93*, LNCS 765, Springer-Verlag, 1993, pp. 386-397.

[6] K. Nyberg, "Linear Approximation of Block Ciphers," *Advances in Cryptology-Eurocrypt'94*, LNCS 950, Springer-Verlag, 1994, pp. 439-444.

[7] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Ohta, "A Strategy for Constructing Fast Round Functions with Practical Security against Differential and Linear Cryptanalysis," *Selected Areas in Cryptography*, LNCS 1556, 1999, pp. 264-279.

[8] K. Aoki and K. Ohta, "Strict Evaluation of the Maximum Average of Differential Probability and the Maximum Average of Linear Probability," *IEICE TRANS. FUNDAMENTALS*, no. 1, 1997, pp. 2-8.

[9] Y. Kaneko, F. Sano, and K. Sakurai, "On Provable Security against Differential and Linear Cryptanalysis in Generalized Feistel Ciphers with Multiple Random Functions," *Proc. of SAC'97*, 1997, pp. 185-199.

[10] M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptalaysis," *Fast Software Encryption*, LNCS 1039, Springer-Verlag, 1996, pp. 205-218.

[11] K. Nyberg and L.R. Knudsen, "Provable Security against Differential Cryptanalysis," *J. of Cryptology*, no. 8, (1), 1995, pp. 27-37.

[12] J. Daemen, L.R. Knudsen, and V. Rijmen, "The Block Cipher SQUARE," *Fast Software Encryption*, LNCS 1267, Springer-Verlag, 1997, pp. 149-165.

[13] L.R. Knudsen, "Practically Secure Feistel Ciphers," *Fast Software Encryption*, LNCS 809, 1994, pp. 211-221.

[14] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E.D. Win,

"The Cipher SHARK," *Fast Software Encryption*, LNCS 1039, Springer-Verlag, 1996, pp. 99-112.

[15] S.H. Hong, S.J. Lee, J.I. Lim, J.C. Sung, and D.H. Choen, "Provable Security against Differential and Linear Cryptanaysis for the SPN structure," *Proc. of FSE2000*, LNCS Springer-Verlag, 1978, pp.273-283.

[16] J.S. Kang, C.S. Park, S.J. Lee, and J.I. Lim, "On the Optimal Diffusion Layer with Practical Security against Differential and Linear Cryptanalysis," *Proc. of ICISC'99*, LNCS 1787, Springer-Verlag, 1999, pp. 38-52.

[17] M. Kanda, "Practical Security Evaluation against Differential and Linear Cryptanalyses for Feistel Ciphers with SPN Round Function," *Selected Areas in Cryptography*, LNCS 2012, Springer-Verlag, 2000, pp. 324-338.

[18] C.H. Lim, "CRYPTON: A New 128-Bit Block Cipher," *AES Proposal*, 1998.

[19] J. Daemen and V. Rijmen, "The Rijndael Block Cipher," *AES Proposal*, 1998.

[20] NTT-Nippon Telegraph and Telephone Corporation, "E2: Efficient Encryption Algorithm," *AES Proposal*, 1998.

[21] F.J. MacWillams and N.J.A. Sloan, *The Theory of Error-Correcting Codes*, NorthHolland, Amsterdam, 1977.

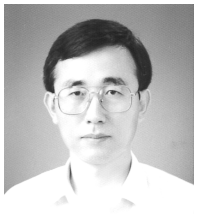
[22] J. Daemen, R. Govaerts, and J. Vandewalle, "Correlation Matrices," *Fast Software Encryption*, LNCS 1008, Springer-Verlag, 1994, pp. 275-285.

Ju-Sung Kang received the B.S., M.S., and Ph.D. degrees in mathematics from Korea University, Seoul, Korea in 1989, 1991, and 1996, respectively. He joined ETRI in 1997, and he is currently with Information Security Division of ETRI. His current research interests include cryptographic algorithms and protocols.

Seokhie Hong received the B.S. and M.S. degrees in mathematics from Korea University. in 1995 and 1997, respectively. He also received the Ph.D. degree in mathematics from Korea University in 2001. Since 2001, he has been with Center for Information Security Technologies (CIST) in Korea University. His current research interests include block cipher analysis and public key cryptosystem.

Sangjin Lee received the B.S. and M.S. degrees in mathematics from Korea University in 1987 and 1989, respectively. He also received the Ph.D. degree in mathematics from Korea University in 1994. From 1989 to 1998, he was a Technical Staff member at ETRI. From 1999 to 2000, he was a faculty member of Mathematics Department at Korea University, and since 2001, he has been an Associate Professor of Graduate School of Information Security. His current research interests include stream cipher and block cipher.

Okyeon Yi received the B.S. and M.S. degrees in Korea University, Seoul, Korea in 1988 and 1990, respectively. He also received the Ph.D. degree in mathematics from University of Kentucky, KY, USA in 1996. He is currently teaching mathematics and cryptology at the Department of Mathematics in Kookmin University, Seoul, Korea. His current research interests include elliptic curve cryptography and information security in IMT-2000.



Choonsik Park received the B.S. degree from Kwangwoon University and the M.S. from Hanyang University, Seoul, Korea in 1981 and 1983, respectively, and the Dr. Eng. degree in electronic engineering from Tokyo Institute of Technology, Tokyo, Japan in 1995. Since joining Coding Technology and Research Section of ETRI in 1982, he has been engaged in research and development on information security. His research interests are information security and cryptographic protocols.

Jongin Lim received the B.S. and M.S. degrees in mathematics from Korea University in 1980 and 1982, respectively. He also received the Ph.D. degree in mathematics from Korea University in 1986. Since joining Korea University in 1986, he was a Professor of Mathematics Department until 2000, and since 2001, he has been a Professor of Graduate School of Information Security. His current research interests include block cipher and public key cryptosystem.