New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis

Mitsuru Matsui

Information Security System Development Center
Mitsubishi Electric Corporation
5-1-1, Ofuna, Kamakura, Kanagawa, 247, Japan
matsui@iss.isl.melco.co.jp

Abstract. We introduce a methodology for designing block ciphers with provable security against differential and linear cryptanalysis. It is based on three new principles: change of the location of round functions, round functions with recursive structure, and substitution boxes of different sizes. The first realizes parallel computation of the round functions without losing provable security, and the second reduces the size of substitution boxes; moreover, the last is expected to make algebraic attacks difficult. We also give specific examples of practical block ciphers that are provably secure under an independent subkey assumption and are reasonably fast in hardware as well as in software implementation.

1 Introduction

In the first version of differential cryptanalysis, the notion "characteristic" was successfully used for breaking block ciphers; if a cipher has a characteristic whose probability is high enough, it is possible to recover some of secret key bits by differential cryptanalysis. On the other hand, Lai, Massey and Murphy [1] found that its converse is not necessarily true, and showed that the notion "differential", instead of characteristic, strictly reflects the strength of a cipher against differential cryptanalysis. Since a differential is, roughly speaking, a collection of characteristics, even if the maximal characteristic probability is low, it cannot be concluded that the cipher is strong against differential cryptanalysis. Meanwhile, Nyberg and Knudsen [2] first showed an example of a block cipher whose maximal differential probability is low enough; they have called such property "provable security" against differential cryptanalysis.

In linear cryptanalysis, we can see a similar situation. The first version of linear cryptanalysis also applied "characteristic" (of linear cryptanalysis) to an attack of block ciphers, but Nyberg [3] has recently showed that a collection of characteristics, which she called "a linear hull", must be taken into consideration for strict evaluation of the strength against linear cryptanalysis. Since the example given in [2] has a low hull probability, it is also provably secure against linear cryptanalysis; however, its computational complexity is not small because it requires a calculation over $GF(2^{33})$.

The purpose of this paper is to discuss a new method for obtaining provably secure and practical block ciphers against differential and linear cryptanalysis. First, we change the location of round functions, which enables their parallel computation without losing provable security. Next, we construct the round functions recursively, which reduces the size of substitution boxes. We also introduce substitution boxes of different sizes, which are expected to increase immunity against possible algebraic attacks; e.g. an explicit description of the entire cipher by a simple algebraic function.

Lastly, we give a full description of two practical examples of block ciphers each of which is provably secure under an independent subkey assumption and is reasonably fast in hardware as well as software implementation. We have confirmed that their software encryption speed is more than 30Mbps on a workstation computer HP9735 (PA7150-125MHz).

2 Security of Substitution Boxes

The purpose of this section and the next section is to give fundamental definitions and lemmas necessary for later sections. We will discuss immunity against differential and linear cryptanalysis in a parallel and self-contained form. The first model in this section is a fixed substitution table S with n input/output bits (figure 1). Throughout this paper, the input bit size of any substitution box is equal to its output bit size. We now start with the following definition.

Definition 1. Let X and Y be a set of possible 2^n input/output patterns of S, respectively. For given $\Delta x, \Gamma x \in X$ and $\Delta y, \Gamma y \in Y$,

$$DP^S(\Delta x \rightarrow \Delta y) \stackrel{def}{=} \frac{\#\{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n}, \tag{1}$$

$$LP^S(\Gamma x \rightarrow \Gamma y) \stackrel{def}{=} \left(2\frac{\#\{x \in X | x \bullet \Gamma x = S(x) \bullet \Gamma y\}}{2^n} - 1\right)^2, \tag{2}$$

where $a \bullet b$ denotes the parity (0 or 1) of bitwise product of a and b.

Note that DP^S and LP^S run from 0 to 1. Although the notation of LP^S is slightly different from a standard definition of linearity, this is convenient for treating differential and linear cryptanalysis in a similar way. Since DP^S and LP^S for a strong substitution box S must be small for any $\Delta x(\neq 0), \Gamma x \in X$ and $\Delta y, \Gamma y(\neq 0) \in Y$, the following parameters represent immunity of S against differential and linear cryptanalysis.

Definition 2.

$$DP^S_{max} \stackrel{def}{=} \max_{\Delta x \neq 0, \Delta y} DP^S(\Delta x \rightarrow \Delta y), \tag{3}$$

$$LP^S_{max} \stackrel{def}{=} \max_{\Gamma x, \Gamma y \neq 0} LP^S(\Gamma x \rightarrow \Gamma y). \tag{4}$$

The following two simple lemmas are useful.

Lemma 3.

$$LP^S(\Gamma x \to \Gamma y) = \left(\sum_{x \in X}{}' (-1)^{x \bullet \Gamma x \oplus S(x) \bullet \Gamma y} \right)^2, \tag{5}$$

where $\sum'_{x \in X}$ *denotes* $\frac{1}{\#X} \sum_{x \in X}$ *and the symbol* $\bullet$ *has higher priority than the symbol* $\oplus$.

Lemma 4. *For any* S,

$$\sum_{\Delta y \in Y} DP^S(\Delta x \to \Delta y) = 1, \tag{6}$$

$$\sum_{\Gamma x \in X} LP^S(\Gamma x \to \Gamma y) = 1. \tag{7}$$

Moreover, if S *is a permutation,*

$$\sum_{\Delta x \in X} DP^S(\Delta x \to \Delta y) = 1, \tag{8}$$

$$\sum_{\Gamma y \in Y} LP^S(\Gamma x \to \Gamma y) = 1. \tag{9}$$

Proof. We show $\sum_{\Gamma x \in X} LP^S(\Gamma x \to \Gamma y) = 1$. The remaining part is then trivial.

$$\begin{aligned}
&\sum_{\Gamma x \in X} LP^S(\Gamma x \to \Gamma y) \\
&= \sum_{\Gamma x \in X} \left(\sum_{x \in X}{}' (-1)^{x \bullet \Gamma x \oplus S(x) \bullet \Gamma y} \right)^2 \\
&= \sum_{\Gamma x \in X} \sum_{x \in X}{}' \sum_{x' \in X}{}' (-1)^{x \bullet \Gamma x \oplus S(x) \bullet \Gamma y \oplus x' \bullet \Gamma x \oplus S(x') \bullet \Gamma y} \\
&= \sum_{x \in X}{}' \sum_{x' \in X}{}' (-1)^{(S(x) \oplus S(x')) \bullet \Gamma y} \sum_{\Gamma x \in X} (-1)^{(x \oplus x') \bullet \Gamma x},
\end{aligned}$$

where the last sum is non-zero if and only if $x = x'$. Hence we easily see that the above must be equal to 1. (QED)

3 Security of Key-Dependent Functions

The next model is a key-dependent function F as shown in figure 2. Let K be a set of all possible key values. We define the strength of F as an average strength of $F < k >$ when k runs over K, where $F < k >$ denotes a one-variable function with the fixed key k. That is:

Definition 5.

$$DP^F(\Delta x \to \Delta y) \stackrel{def}{=} \sum_{k \in K}{}' DP^{F<k>}(\Delta x \to \Delta y), \tag{10}$$

$$LP^F(\Gamma x \to \Gamma y) \stackrel{def}{=} \sum_{k \in K}{}' LP^{F<k>}(\Gamma x \to \Gamma y). \tag{11}$$

In particular, when F is an encryption function, and DP^F and LP^F are small enough for any $\Delta x(\neq 0), \Gamma x \in X$ and $\Delta y, \Gamma y(\neq 0) \in Y$, we say that F is provably secure against differential and linear cryptanalysis. Equivalently, F has provable security if the following values are small:

Definition 6.

$$DP^F_{max} \stackrel{def}{=} \max_{\Delta x \neq 0, \Delta y} DP^F(\Delta x \to \Delta y), \tag{12}$$

$$LP^F_{max} \stackrel{def}{=} \max_{\Gamma x, \Gamma y \neq 0} LP^F(\Gamma x \to \Gamma y). \tag{13}$$

In the rest of this section, we consider two cases where the key-dependent function F has a special form (figures 3 and 4). The following fundamental theorem shows that average strength of the entire cipher is represented by a collection of all possible "probabilistic paths", where the first equality was proved by Lai, Massey and Murphy [1], and the second by Nyberg [3]. Though their original papers have wider frameworks, we here give a direct proof for our convenience.

Theorem 7 [1][3]. *For the function F shown in figure 3,*

$$DP^F(\Delta x \to \Delta z) = \sum_{\Delta y \in Y} DP^{S_1}(\Delta x \to \Delta y) DP^{S_2}(\Delta y \to \Delta z) \tag{14}$$

$$LP^F(\Gamma x \to \Gamma z) = \sum_{\Gamma y \in Y} LP^{S_1}(\Gamma x \to \Gamma y) LP^{S_2}(\Gamma y \to \Gamma z). \tag{15}$$

Proof. Since clearly $k_1 \in K_1$ does not affect the conclusion, we neglect k_1. For the first equality,

$$\begin{aligned} & DP^F(\Delta x \to \Delta z) \\ &= \sum_{k_2 \in K_2}{}' \sum_{\Delta y \in Y} DP^{S_1}(\Delta x \to \Delta y) \widetilde{DP}^{F_2<k_2>}(\Delta y \to \Delta z | \Delta x \to \Delta y) \\ &= \sum_{\Delta y \in Y} DP^{S_1}(\Delta x \to \Delta y) \sum_{k_2 \in K_2}{}' \widetilde{DP}^{F_2<k_2>}(\Delta y \to \Delta z | \Delta x \to \Delta y), \end{aligned} \tag{16}$$

where the last term represents a conditional probability that Δy results in Δz when Δx causes Δy. In other words, there exists a subset $\tilde{Y}$ of Y,

$$\begin{aligned} & \widetilde{DP}^{F_2<k_2>}(\Delta y \to \Delta z | \Delta x \to \Delta y) \\ &= \#\{\tilde{y} \in \tilde{Y} | F_2 < k_2 > (\tilde{y}) \oplus F_2 < k_2 > (\tilde{y} \oplus \Delta y) = \Delta z\} / \#\tilde{Y}. \end{aligned}$$

Therefore the second sum of (16) is

$$\begin{aligned}
&\sum_{k_2 \in K_2}{}' DP^{F_2<k_2>}(\Delta y \rightarrow \Delta z | \Delta x \rightarrow \Delta y) \\
&= \sum_{k_2 \in K_2}{}' \#\{\tilde{y} \in \tilde{Y} | F_2 < k_2 > (\tilde{y}) \oplus F_2 < k_2 > (\tilde{y} \oplus \Delta y) = \Delta z\} / \#\tilde{Y} \\
&= \sum_{k_2 \in K_2}{}' \#\{\tilde{y} \in \tilde{Y} | S_2(\tilde{y} \oplus k_2) \oplus S_2(\tilde{y} \oplus k_2 \oplus \Delta y) = \Delta z\} / \#\tilde{Y} \\
&= \sum_{\tilde{y} \in \tilde{Y}}{}' \#\{k_2 \in K_2 | S_2(\tilde{y} \oplus k_2) \oplus S_2(\tilde{y} \oplus k_2 \oplus \Delta y) = \Delta z\} / \#\tilde{K}_2 \\
&= \sum_{\tilde{y} \in \tilde{Y}}{}' DP^{S_2}(\Delta y \rightarrow \Delta z) \\
&= DP^{S_2}(\Delta y \rightarrow \Delta z).
\end{aligned}$$

For the second equality,

$$\begin{aligned}
&\sum_{\Gamma y \in Y} LP^{S_1}(\Gamma x \rightarrow \Gamma y) LP^{S_2}(\Gamma y \rightarrow \Gamma z) \\
&= \sum_{\Gamma y \in Y} \sum_{x \in X}{}' \sum_{x' \in X}{}' \sum_{y \in Y}{}' \sum_{y' \in Y}{}' \\
&\quad (-1)^{x \bullet \Gamma x \oplus S_1(x) \bullet \Gamma y \oplus x' \bullet \Gamma x \oplus S_1(x') \bullet \Gamma y \oplus y \bullet \Gamma y \oplus S_2(y) \bullet \Gamma z \oplus y' \bullet \Gamma y \oplus S_2(y') \bullet \Gamma z} \\
&= \sum_{x \in X}{}' \sum_{x' \in X}{}' \sum_{y \in Y}{}' \sum_{y' \in Y}{}' (-1)^{x \bullet \Gamma x \oplus x' \bullet \Gamma x \oplus S_2(y) \bullet \Gamma z \oplus S_2(y') \bullet \Gamma z} \times \\
&\quad \sum_{\Gamma y \in Y} (-1)^{(S_1(x) \oplus S_1(x') \oplus y \oplus y') \bullet \Gamma y},
\end{aligned}$$

where the last sum is nonzero if and only if $S_1(x) \oplus S_1(x') \oplus y \oplus y' = 0$. Hence by eliminating y' and substituting k_2 for y we obtain

$$\begin{aligned}
&= \sum_{x \in X}{}' \sum_{x' \in X}{}' \sum_{k_2 \in K_2}{}' (-1)^{x \bullet \Gamma x \oplus x' \bullet \Gamma x \oplus S_2(k_2) \bullet \Gamma z \oplus S_2(k_2 \oplus S_1(x) \oplus S_1(x')) \bullet \Gamma z} \\
&= \sum_{x \in X}{}' \sum_{x' \in X}{}' \sum_{k_2 \in K_2}{}' (-1)^{x \bullet \Gamma x \oplus x' \bullet \Gamma x \oplus S_2(k_2 \oplus S_1(x)) \bullet \Gamma z \oplus S_2(k_2 \oplus S_1(x')) \bullet \Gamma z} \\
&= \sum_{k_2 \in K_2}{}' LP^{F<k_2>}(\Gamma x \rightarrow \Gamma z) \\
&= LP^{F}(\Gamma x \rightarrow \Gamma z). \quad (QED)
\end{aligned}$$

Note that the above theorem assumes that S_1 and S_2 are fixed substitution tables. However we can extend them to key-dependent functions as follows.

Theorem 8. *For the function F shown in figure 4,*

$$DP^F(\Delta x \to \Delta z) = \sum_{\Delta y \in Y} DP^{F_1}(\Delta x \to \Delta y) DP^{F_2}(\Delta y \to \Delta z), \tag{17}$$

$$LP^F(\Gamma x \to \Gamma z) = \sum_{\Gamma y \in Y} LP^{F_1}(\Gamma x \to \Gamma y) LP^{F_2}(\Gamma y \to \Gamma z). \tag{18}$$

Proof. We show the first equality. The second can be similarly derived.

$$\begin{aligned} & DP^F(\Delta x \to \Delta z) \\ &= \sum_{ki_1 \in KI_1}{}' \sum_{ki_1 \in KI_1}{}' \sum_{ko_1 \in KO_1}{}' \sum_{ko_2 \in KO_2}{}' DP^{F<ki_1, ki_2, ko_1, ko_2>}(\Delta x \to \Delta z). \end{aligned}$$

By using theorem 7 for fixed ki_1 and ki_2, we have

$$\begin{aligned} &= \sum_{ki_1 \in KI_1}{}' \sum_{ki_2 \in KI_2}{}' \sum_{\Delta y \in Y} DP^{F_1<ki_1>}(\Delta x \to \Delta y) DP^{F_2<ki_2>}(\Delta y \to \Delta z) \\ &= \sum_{\Delta y \in Y} \sum_{ki_1 \in KI_1}{}' DP^{F_1<ki_1>}(\Delta x \to \Delta y) \sum_{ki_2 \in KI_2}{}' DP^{F_2<ki_2>}(\Delta y \to \Delta z) \\ &= \sum_{\Delta y \in Y} DP^{F_1}(\Delta x \to \Delta y) DP^{F_2}(\Delta y \to \Delta z). \quad (QED) \end{aligned}$$

The following corollary shows that an $(n+1)$-round cipher is not "weaker" than an n-round cipher with the same round functions.

Corollary 9. *For the function F shown in figure 4,*

$$DP^F_{max} \le DP^{F_1}_{max} + DP^{F_2}_{max}, \tag{19}$$

$$LP^F_{max} \le LP^{F_1}_{max} + LP^{F_2}_{max}. \tag{20}$$

Moreover, if F is bijective for any key value,

$$DP^F_{max} \le min\{DP^{F_1}_{max}, DP^{F_2}_{max}\}, \tag{21}$$

$$LP^F_{max} \le min\{LP^{F_1}_{max}, LP^{F_2}_{max}\}. \tag{22}$$

Proof. We show the first inequality. The remaining part can be similarly proved. For any $\Delta x \neq 0$ and Δz, we have, by lemma 4 and theorem 8,

$$\begin{aligned} & DP^F(\Delta x \to \Delta z) \\ &= \sum_{\Delta y \in Y \setminus \{0\}} DP^{F_1}(\Delta x \to \Delta y) DP^{F_2}(\Delta y \to \Delta z) + DP^{F_1}(\Delta x \to 0) DP^{F_2}(0 \to \Delta z) \\ &\le \sum_{\Delta y \in Y \setminus \{0\}} DP^{F_1}(\Delta x \to \Delta y) DP^{F_2}_{max} + DP^{F_1}_{max} \\ &\le DP^{F_1}_{max} + DP^{F_2}_{max}. \quad (QED) \end{aligned}$$

4 New Structure of Block Ciphers with Provable Security

In [2], Nyberg and Knudsen first showed an example of a DES-like block cipher with provable security against differential cryptanalysis. Nyberg also showed in [3] that this example also has provable security against linear cryptanalysis. Its principle is based on the following theorem.

Theorem 10 [2][3]. *For the n-round ($n \geq 3$) function F given in figure 5, assume that each substitution box S_i is bijective and $DP^{S_i}_{max} \leq p$ (resp. $LP^{S_i}_{max} \leq p$). Then $DP^F_{max} \leq 2p^2$ (resp. $LP^F_{max} \leq 2p^2$).*

Example 1. In figure 5, let S_i be a cubic function of galois field $GF(2^{32})$. Then since $DP^{S_i}_{max} = LP^{S_i}_{max} = 2^{-30}$, $DP^F_{max} \leq 2^{-59}$ and $LP^F_{max} \leq 2^{-59}$.
(For a cubic function f over $GF(2^n)$, if n is even $DP^f_{max} = LP^f_{max} = 2^{-n+2}$, and if n is odd $DP^f_{max} = LP^f_{max} = 2^{-n+1}$. see [4].)

The purpose of the remaining part of this section is to discuss various extensions of theorem 10. First, we change the location of the substitution boxes as in figure 6. Then we can prove the following.

Theorem 11. *For the n-round ($n \geq 3$) function F given in figure 6, assume that each substitution box S_i is bijective and $DP^{S_i}_{max} \leq p$ (resp. $LP^{S_i}_{max} \leq p$). Then $DP^F_{max} \leq p^2$ (resp. $LP^F_{max} \leq p^2$).*

Proof. We prove the theorem when $n = 3$. The case $n > 3$ is then trivial using corollary 9. We consider four cases:

Case 1: If $\Delta x^R = 0$, then $\Delta x^L \neq 0$. Hence

$$\begin{aligned} & DP^F(\Delta x \rightarrow \Delta y) \\ &= DP^{S_2}(\Delta x^L \rightarrow \Delta x^L \oplus \Delta y^R) DP^{S_3}(\Delta x^L \rightarrow \Delta y^L \oplus \Delta y^R) \\ &\leq DP^{S_2}_{max} DP^{S_3}_{max} = p^2. \end{aligned}$$

Case 2: If $\Delta x^L = 0$, then $\Delta x^R \neq 0$. The output difference of S_2 is zero and the input difference of S_3 must be equal to Δy^R; hence $\Delta y^R \neq 0$.

$$\begin{aligned} & DP^F(\Delta x \rightarrow \Delta y) \\ &= DP^{S_1}(\Delta x^R \rightarrow \Delta y^R) DP^{S_3}(\Delta y^R \rightarrow \Delta y^L \oplus \Delta y^R) \\ &\leq DP^{S_1}_{max} DP^{S_3}_{max} = p^2. \end{aligned}$$

Case 3: If $\Delta y^L \oplus \Delta y^R = 0$, then the input difference of S_3 is zero and the output difference of S_1 must be equal to Δx^L. Hence $\Delta x^L \neq 0$ and $\Delta x^R \neq 0$.

$$\begin{aligned} & DP^F(\Delta x \rightarrow \Delta y) \\ &= DP^{S_1}(\Delta x^R \rightarrow \Delta x^L) DP^{S_2}(\Delta x^L \rightarrow \Delta y^R) \\ &\leq DP^{S_1}_{max} DP^{S_2}_{max} = p^2. \end{aligned}$$

Case 4: Otherwise, let the output difference of S_1 be $\Delta\alpha$, which is not determined uniquely. By a similar method to the proof of theorem 7, we have

$$\begin{aligned}
&DP^F(\Delta x \to \Delta y) \\
&= \sum_{\Delta\alpha} DP^{S_1}(\Delta x^R \to \Delta\alpha) DP^{S_2}(\Delta x^L \to \Delta x^L \oplus \Delta y^R \oplus \Delta\alpha) \times \\
&\quad DP^{S_3}(\Delta x^L \oplus \Delta\alpha \to \Delta y^L \oplus \Delta y^R) \\
&\le DP^{S_1}_{max} DP^{S_2}_{max} \sum_{\Delta\alpha} DP^{S_3}(\Delta x^L \oplus \Delta\alpha \to \Delta y^L \oplus \Delta y^R) \\
&= DP^{S_1}_{max} DP^{S_2}_{max} = p^2.
\end{aligned}$$

Theorem 11 shows that figure 6 is structurally stronger than figure 5 concerning to both differential and linear cryptanalysis under the condition that all S_i's are bijective. It should be also noted that in figure 6 two neighboring substitution boxes are parallelizable. Moreover, this theorem is valid even if the substitution boxes are affected by the secret key as in figure 7. That is, the following theorem holds, which enables us to construct round functions recursively. Its proof can be done in the same way.

Theorem 12. *For the n-round ($n \ge 3$) function F given in figure 7, assume that each function F_i is bijective for any key and $DP^{F_i}_{max} \le p$ (resp. $LP^{F_i}_{max} \le p$). Then $DP^F_{max} \le p^2$ (resp. $LP^F_{max} \le p^2$).*

Example 2. In figure 7, assume that F_i has a structure shown in figure 6 and let $S_{i,j}$ (the j-th substitution box in F_i) be a cubic function of $GF(2^{16})$. Then since $DP^{S_i}_{max} = LP^{S_i}_{max} = 2^{-14}$, $DP^F_{max} \le (DP^{F_i}_{max})^2 \le (DP^{S_{i,j}}_{max})^4 = 2^{-56}$ and similarly, $LP^F_{max} \le 2^{-56}$.

Lastly, we can extend theorem 12 to the case where the bit size of X^L is not necessarily the same as that of X^R.

Theorem 13. *For the n-round ($n \ge 3$) function F given in figure 7, let the bit size of X^L and X^R be n and m ($n \le m$), respectively. We assume that at the first and third XORs, the left n-bit data is zero-extended to m-bit, and at the second XOR the left m-bit data is truncated to n-bit. If each function F_i is bijective for any key, then we have*

$$DP^F_{max} \le max\{DP^{F_1} DP^{F_2}, DP^{F_2} DP^{F_3}, 2^{m-n} DP^{F_1} DP^{F_3}\}, \quad (23)$$

$$LP^F_{max} \le max\{LP^{F_1} LP^{F_2}, LP^{F_2} LP^{F_3}, 2^{m-n} LP^{F_1} LP^{F_3}\}. \quad (24)$$

Proof. The difference from the proof of theorem 11 is "Case 2" only. In this case, since only lower n bits of $\Delta\alpha$ are determined uniquely, the number of possible $\Delta\alpha$ is 2^{m-n}. (QED)

Example 3. In figure 7, assume that F_i has the structure shown in figure 6, where 32-bit input data of F_i is divided into 15-bit and 17-bit data. Let S_{i1} and S_{i3} be cubic functions of $GF(2^{17})$ and S_{i2} be a cubic function of $GF(2^{15})$. Then since $DP^{F_i}_{max} = LP^{F_i}_{max} = 2^{-30}$ due to theorem 13, $DP^F_{max} \le (DP^{F_i}_{max})^2 = 2^{-60}$. Similarly we have $LP^F_{max} \le 2^{-60}$.

5 Examples

In this section we presents two specific examples of 64-bit block ciphers that are provably secure under an independent key assumption and are practically fast. Figures 8 to 12 and tables 1 to 2 show their full description, where "left" means "lower address".

- Figures 8 and 9 show data randomization parts of the two ciphers, each of which contains two types of common sub functions FO_i $(1 \leq i \leq 8)$ and FL_i $(1 \leq i \leq 10)$. FO_i uses two 48-bit subkeys KI_i and KO_i, and FL_i uses a 32-bit subkey KL_i.
- Figure 10 shows the structure of FO_i (the first level recursive function), which contains three sub functions $FI_{i,j}$ $(1 \leq j \leq 3)$. $KO_{i,j}$ and $KI_{i,j}$ are the j-th 16-bit data of KO_i and KI_i, respectively.
- Figure 11 shows the structure of $FI_{i,j}$ (the second level recursive function), which contains two types of substitution boxes S_7 and S_9. The input of $FI_{i,j}$ is divided into left 9-bit data and right 7-bit data. Accordingly, $KI_{i,j}$ is divided into left 7-bit $KI_{i,j,1}$ and right 9-bit data $KI_{i,j,2}$.
- Tables 1 and 2 show decimal representation of substitution boxes S_7 and S_9, respectively. S_7 is affine equivalent to a 17-th power function on $GF(2^7)$ and S_9 is to a 5-th power function on $GF(2^9)$. Note that, similarly to a cubic function, we obtain $DP_{max}^{S_7} = LP_{max}^{S_7} = 2^{-6}$ and $LP_{max}^{S_9} = LP_{max}^{S_9} = 2^{-8}$. The choice of these tables is due to a purely hardware reason; we omit the detail due to space constraints.
- Figure 12 shows the structure of FL_i, where $KL_{i,j}$ is the j-th 16-bit data of KL_i $(1 \leq j \leq 2)$. $\cap$ and $\cup$ denote bitwise AND and OR operations, respectively.

We easily see, using theorem 13, that each cipher has the following security parameters. It should be noted that since the FL_i is a linear function for each fixed key, it does not affect their security:

$$DP_{max}^{figure8} \leq 2^{-55}, \quad LP_{max}^{figure8} \leq 2^{-55},$$
$$DP_{max}^{figure9} \leq 2^{-56}, \quad LP_{max}^{figure9} \leq 2^{-56}.$$

As for their encryption performance, the first cipher can execute two $FI_{i,j}$ in parallel, and the second can process four in parallel. In figure 9, for example, $FI_{1,1}$, $FI_{1,2}$, $FI_{2,1}$, $FI_{2,2}$ are parallelizable. The same is true for $FI_{1,3}$, $FI_{2,3}$, $FI_{3,1}$, $FI_{4,1}$ and $FI_{3,2}$, $FI_{3,3}$, $FI_{4,2}$, $FI_{4,3}$. In hardware implementation, therefore, the second cipher is expected to be twice as fast as the first cipher. In software, our computer program successfully encodes plaintext at a speed of more than 30Mbps for either algorithm on a workstation computer HP9735 (PA7150-125MHz).

We should also notice that although the decryption speed of the first cipher is the same as its encryption speed, the decryption speed of the second cipher is slower than its encryption in ECB and CBC modes. Therefore the second should be used in OFB or CFB modes.

Lastly, we show an example of the common (and simple) key schedule part when the bit size of the secret key K is 128.

- The secret key K is divided into eight 16-bit data K_i $(1 \leq i \leq 8)$.
- Let K_{i+8} be the output of FI with $KI = 0$ for input K_i $(1 \leq i \leq 8)$.
- The correspondence between the secret key and the subkeys is as follows:

i	1	2	3	4	5	6	7	8	9	10
$KL_{i,1}$	K_2	K_4	K_{16}	K_{10}	K_6	K_8	K_{12}	K_{14}	K_2	K_4
$KL_{i,2}$	K_1	K_3	K_{15}	K_9	K_5	K_7	K_{11}	K_{13}	K_1	K_3

i	1	2	3	4	5	6	7	8
$KO_{i,1}$	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
$KI_{i,1}$	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_9	K_{10}
$KO_{i,2}$	K_4	K_5	K_6	K_7	K_8	K_1	K_2	K_3
$KI_{i,2}$	K_{15}	K_{16}	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}
$KO_{i,3}$	K_6	K_7	K_8	K_1	K_2	K_3	K_4	K_5
$KI_{i,3}$	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_9

Test data are as follows:

Secret Key (K_1 to K_8)	`0011 2233 4455 6677 8899 aabb ccdd eeff`
Plaintext	`0123 4567 89ab cdef`
K_9 to K_{16}	`f28d c826 ddf9 e1c7 439a 05b7 8c23 cdce`
Ciphertext (Algorithm I)	`787a 62bb f622 6cd6`
Ciphertext (Algorithm II)	`bfbf 3940 217d 4252`

References

1. Lai, X., Massey, J.L., Murphy, S.,: Markov Ciphers and Differential Cryptanalysis. Advances in Cryptology – Eurocrypt'91, Lecture Notes in Computer Science **547**, Springer-Verlag (1991)
2. Nyberg, K., Knudsen, L.,: Provable Security against Differential Cryptanalysis. Journal of Cryptology, Vol.8, no.1 (1995)
3. Nyberg, K.,: Linear Approximation of Block Ciphers. Advances in Cryptology – Eurocrypt'94, Lecture Notes in Computer Science **950**, Springer-Verlag (1994)
4. Nyberg, K.,: Differential Uniform Mappings for Cryptography. Advances in Cryptology – Eurocrypt'93, Lecture Notes in Computer Science **765**, Springer-Verlag (1993)

```
S7[128] = {
 85, 95, 53, 57, 65, 63, 99, 27, 86, 31, 33,110, 18, 47, 39, 28,
 29, 61, 37,  3, 66, 22, 56,106, 15,108, 32, 69,  0, 23,109,124,
101, 96, 97, 98, 64, 49,  6,113, 30, 88, 13, 77,107, 89, 58, 14,
 36, 11,120, 81, 74, 17, 84,  9, 78, 34,  5,111,112,104,121,103,
 80,126, 90,114, 82,  8, 26, 70, 94, 51, 67, 40, 12, 21, 83, 76,
 45, 41,127,125,100, 20,116,  2, 50,117,119, 54, 43, 24, 44, 25,
 72,105, 38,  1,123, 46, 87,  4, 62, 92, 71, 35, 93, 75,102,118,
 60, 55, 10,  7, 68, 59, 48, 73, 91, 19,122, 52,115, 79, 16, 42 };
```

Table 1: The table of S_7.

```
S9[512] = {
341,310, 37,213, 79,140,348,268,379,262,266,484,273,460,259,333,
241,402,295,215,419, 96, 22,326,453,184,274,252,487, 58,339, 29,
220,255,420,276,103,228,380,364,230,219,159, 49,301,432,311,313,
342,117,136,312,421, 38, 24,264,118,331,169,263,501,104,329, 71,
280,472,120, 43,  6,102,261,502,127,161, 30, 83, 17,111, 19,254,
 62,510,504,171,360,  8,205,318, 67,413,132,457,101,283,193,300,
309,437, 93, 78,394,426,129, 50, 70,216, 47, 34,393,439,387,302,
 61,445,499,224,202,490,359,212, 84,458,155,406,467,237,383,210,
385,506,400,376,153, 66,235,163,303,330, 63,201,327,386, 52, 98,
121,258,206,294,297,242,509,181,461,168,123,397,493, 40, 56,366,
 41, 18, 48,152,144, 11,234,226,147,182,395,317,346,479, 33, 55,
511,196,320,232,270,149,466,218, 95,378,481, 87,478, 91,  3,277,
 69,157, 68, 15,345,289,315,464,418,356,162,247,462,424,173, 88,
319,231,408,211,107,275,175,324,450,  4,100,305,486,128, 35,470,
 73,209, 64, 75,244,204,158, 53,442,316,178,167,119, 81,284,425,
285,133,434,185,488,208,292,143,500,114, 90,335,113,343,444,  9,
454,369,176,148,388,403,145, 21,456,353,447,389,250,243,238,116,
 99,468,435,151,105,382,474, 94,375,222,422,156, 13,260,191,293,
217, 46,423,451,314,365, 39,227,195, 42,188,198, 80, 25, 76,150,
338,165,138,494,249,430,322,134, 82,443,139,497,137,448, 51,489,
203,223,429,298,141, 57,392,431,396,390,491,370,186, 16,190,135,
492,248, 44,427,482, 86, 65,358,433,187,368,233,207,357,109,340,
112, 36,286,473,407,355,154,253,291,361,332,405,436,350,440,449,
377, 45,177,374,214,290,381, 26,304,122,505, 32,495,  5,325, 60,
351,496,328,372,287,272,363,503,465,352,199,229,225,240,404,278,
166,265, 23,299,174,417,124,480,306,131,130,416, 74,347,409, 27,
 97,142,126,  2,384,463,508,288,251, 10,485,391,106, 59,279,469,
438, 89,271,115, 31,336,197,281, 54,455,398,236,239,446,308,246,
475,471,476,323,415,307,507,452, 28, 14,282,411,296,410, 77,108,
160,428,  1,414,172,256,110,337,125,367,477, 92,257,179,194,483,
321,269,334,401,164, 72,200,183,146,192,412,349,  7,245,362,267,
 20,344,189,354,441, 85,371, 12,221,399,373,180,  0,498,459,170 };
```

Table 2: The table of S_9.

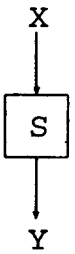

Figure 1

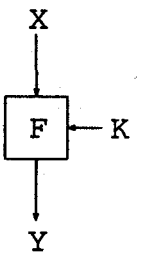

Figure 2

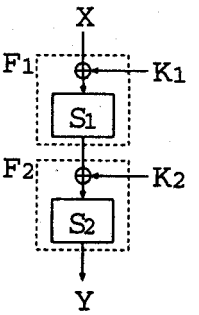

Figure 3

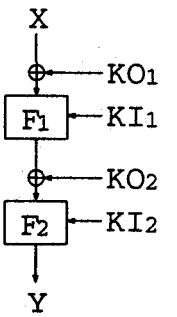

Figure 4

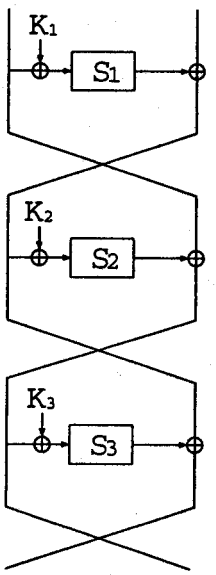

Figure 5

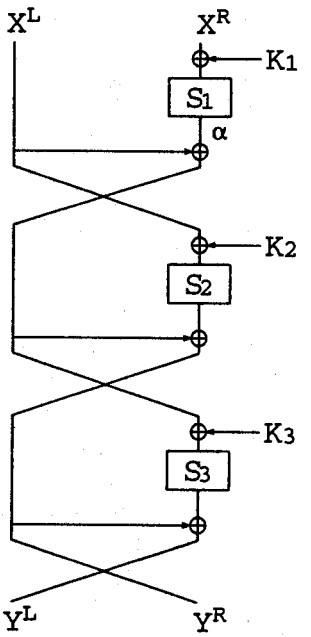

Figure 6

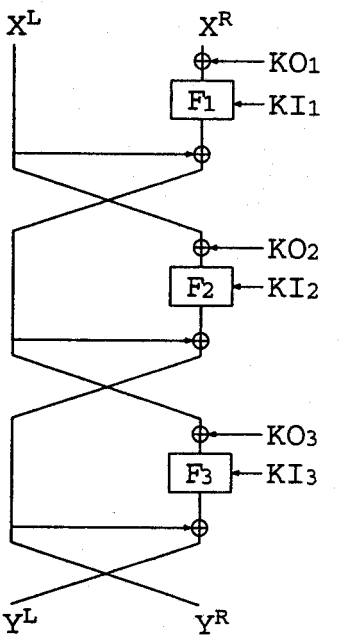

Figure 7

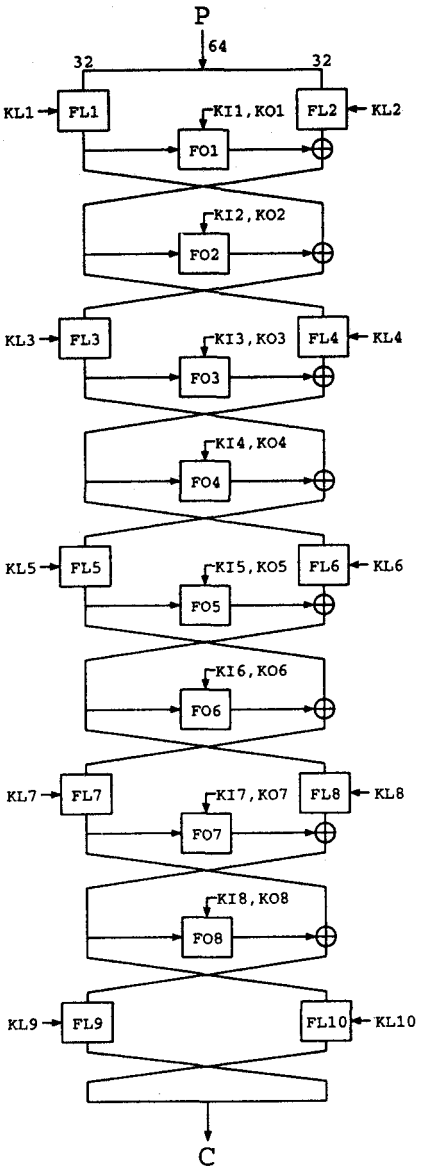

Figure 8: Algorithm I

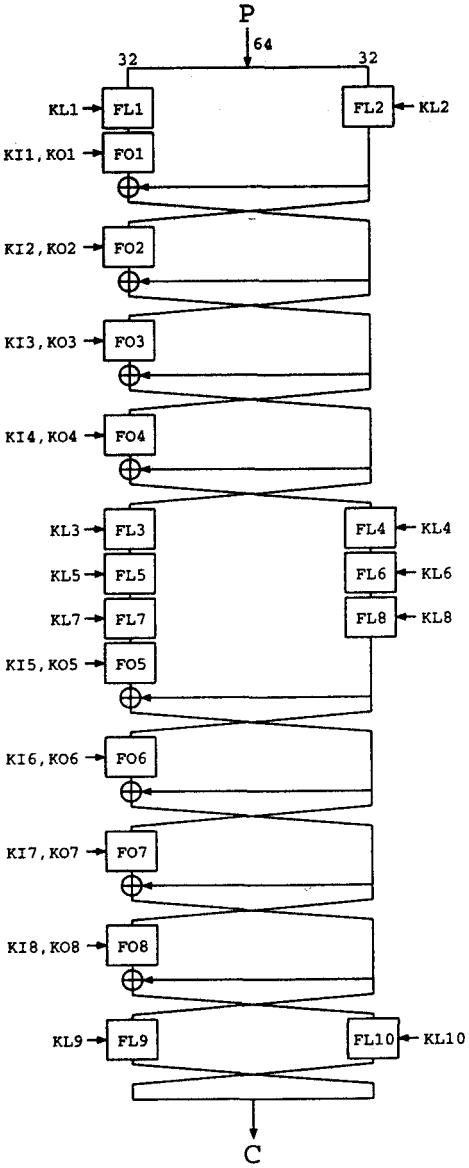

Figure 9: Algorithm II

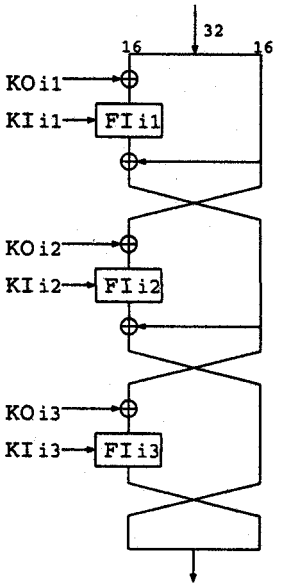

Figure 10: FOi

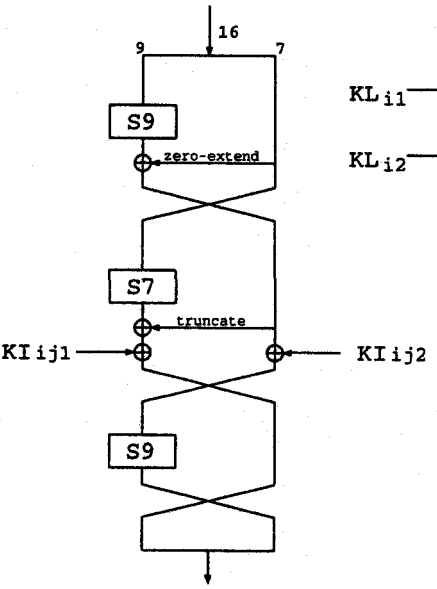

Figure 11: FIij

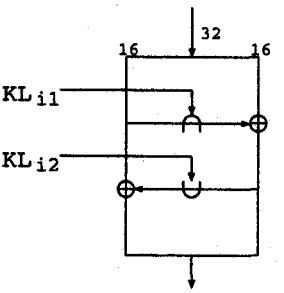

Figure 12: FLi