Linear Cryptanalysis Method for DES Cipher

Mitsuru Matsui

Computer & Information Systems Laboratory
Mitsubishi Electric Corporation
5-1-1, Ofuna, Kamakura, Kanagawa 247, Japan
E-mail matsui@mmt.isl.melco.co.jp

Abstract

We introduce a new method for cryptanalysis of DES cipher, which is essentially a known-plaintext attack. As a result, it is possible to break 8-round DES cipher with 2^{21} known-plaintexts and 16-round DES cipher with 2^{47} known-plaintexts, respectively. Moreover, this method is applicable to an only-ciphertext attack in certain situations. For example, if plaintexts consist of natural English sentences represented by ASCII codes, 8-round DES cipher is breakable with 2^{29} ciphertexts only.

1 Introduction

Differential Cryptanalysis has been one of main topics in cryptology since the first paper by Biham and Shamir in 1990 [1]. They have broken FEAL cipher in the subsequent paper [2], and recently succeeded in breaking the full 16-round DES cipher by a chosen-plaintext attack [3].

Although Differential Cryptanalysis is a technique for a chosen-plaintext attack, it is more noteworthy that it can be applied to a known-plaintext attack on condition that sufficiently many plaintexts are available.

On the other hand, several new approaches to known-plaintext attacks have been also studied in special cases. As regards FEAL cipher, for example, Tardy-Corfdir and Gilbert have presented a statistical method to break FEAL-4 and FEAL-6 [4], and Matsui and Yamagishi have described a deterministic method to break FEAL-8 by a known-plaintext attack [5], respectively.

In this paper we introduce an essentially known-plaintext attack of DES cipher. The purpose of this method is to obtain a linear approximate expression of a given cipher algorithm. For this purpose, we begin by constructing a statistical linear path between input and output bits of each S-box. Then we extend this path to the entire algorithm, and finally reach a linear approximate expression without any intermediate value.

Our main results on the known-plaintext attack of DES cipher are as follows. The experiments were implemented with C language programs on HP9750 workstation computer (PA-RISC/66MHz).

- 8-round DES is breakable with 2^{21} known-plaintexts in 40 seconds;
- 12-round DES is breakable with 2^{33} known-plaintexts in 50 hours;
- 16-round DES is breakable with 2^{47} known-plaintexts faster than an exhaustive search for 56 key bits.

Generally speaking, there exist many linear approximate expressions for a given cipher algorithm. Moreover, if plaintexts are not random, we may even find an expression which has no plaintext bit in it. This suggests that our method finally leads to an only-ciphertext attack. As regards the only-ciphertext attack of DES cipher, we have obtained the following results.

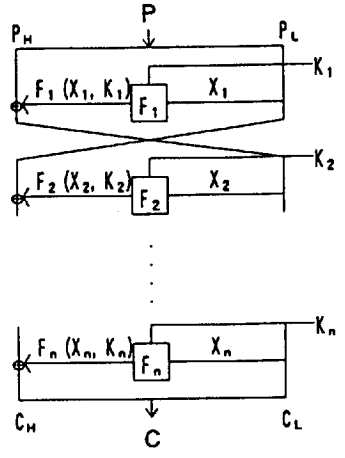
- If plaintexts consist of natural English sentences represented by ASCII codes, 8-round DES is breakable with 2^{29} ciphertexts only;
- If plaintexts consist of random ASCII codes, 8-round DES is breakable with 2^{37} ciphertexts only.

We shall also illustrate a situation in which 16-round DES is still breakable faster than an exhaustive search for 56-bit keys by the only-ciphertext attack.

2 Preliminaries

Figure 1 shows a data randomization part of DES cipher. We omit the initial permutation IP and the final permutation IP^{-1} unless otherwise indicated. The following notations are used throughout this paper, where the right most bit is referred to as the zero-th bit.

P : The 64-bit plaintext.
C : The corresponding 64-bit ciphertext.
P_H : The left 32-bit of P.
P_L : The right 32-bit of P.
C_H : The left 32-bit of C.
C_L : The right 32-bit of C.
X_i : The 32-bit intermediate value in the i-th round.
K_i : The 48-bit subkey in the i-th round.
$F_i(X_i, K_i)$: The i-th round F-function.
$A[i]$: The i-th bit of A.
$A[i, j, ..., k]$: $A[i] \oplus A[j] \oplus, ..., \oplus A[k]$.



[Fig. 1] DES cipher

3 Principle of Linear Cryptanalysis

The purpose of Linear Cryptanalysis is to find the following "effective" linear expression for a given cipher algorithm:

$$P[i_1, i_2, .., i_a] \oplus C[j_1, j_2, .., j_b] = K[k_1, k_2, .., k_c], \quad (1)$$

where $i_1, i_2, .., i_a, j_1, j_2, .., j_b$ and $k_1, k_2, .., k_c$ denote fixed bit locations, and equation (1) holds with probability $p \neq 1/2$ for randomly given plaintext P and the corresponding ciphertext C. The magnitude of $|p - 1/2|$ represents the effectiveness of equation (1).

Once we succeed in reaching an effective linear expression, it is possible to determine one key bit $K[k_1, k_2, .., k_c]$ by the following algorithm based on the maximum likelihood method:

Algorithm 1

Step1 Let T be the number of plaintexts such that the left side of equation (1) is equal to zero.

Step2 If $T > N/2$ (N denotes the number of plaintexts),
then guess $K[k_1, k_2, .., k_c] = 0$ (when $p > 1/2$) or 1 (when $p < 1/2$),
else guess $K[k_1, k_2, .., k_c] = 1$ (when $p > 1/2$) or 0 (when $p < 1/2$).

The success rate of this method clearly increases when N or $|p - 1/2|$ does. We now refer to the most effective linear expression (i.e. $|p - 1/2|$ is maximal) as the best expression and the probability p as the best probability. Then our main concern is the following:

P1 How to find effective linear expressions.

P2 An explicit description of the success rate by N and p.

P3 A search for the best expression and a calculation of the best probability.

The first aim of this paper is to solve these problems for DES cipher. For this purpose, we begin by studying linear approximations of S-boxes in Chapter 4, and will reach an effective linear expression in Chapter 5. In this stage, the success rate will be also shown in Lemma 2. As for the search problem, which was solved by a computer program, we summarize the results in the annex.

For a practical known-plaintext attack of n-round DES cipher, we make use of the best expression of $(n-1)$-round DES cipher; that is to say, regarding the final round as having been deciphered using K_n, we accept a term of F-function in the linear expression. Consequently, we obtain the following type of expression which holds with the best probability of $(n-1)$-round DES cipher:

$$P[i_1, i_2, .., i_a] \oplus C[j_1, j_2, .., j_b] \oplus F_n(C_L, K_n)[l_1, l_2, .., l_d] = K[k_1, k_2, .., k_c]. \quad (2)$$

If one substitutes an incorrect candidate for K_n in equation (2), the effectiveness of this equation clearly decreases. Therefore, the following maximum likelihood method can be applied to deduce K_n and $K[k_1, k_2, .., k_c]$:

Algorithm 2

Step1 For each candidate $K_n^{(i)}$ $(i = 1, 2, ...)$ of K_n, let T_i be the number of plaintexts such that the left side of equation (2) is equal to zero.

Step2 Let T_{max} be the maximal value and T_{min} be the minimal value of all T_i's.

- If $|T_{max} - N/2| > |T_{min} - N/2|$, then adopt the key candidate corresponding to T_{max} and guess $K[k_1, k_2, .., k_c] = 0$ (when $p > 1/2$) or 1 (when $p < 1/2$).
- If $|T_{max} - N/2| < |T_{min} - N/2|$, then adopt the key candidate corresponding to T_{min} and guess $K[k_1, k_2, .., k_c] = 1$ (when $p > 1/2$) or 0 (when $p < 1/2$).

The success rate of this method will be discussed in Lemma 4 and Lemma 5.

The next aim of this paper is to consider the case where plaintexts are not random. Assume that, for example, the probability that $P[i_1, i_2, .., i_a] = 0$ is not equal to 1/2. Then even if we eliminate the term $P[i_1, i_2, .., i_a]$ from equation (2), the resultant equation may be still effective. This concludes that Algorithm 2 can be directly applied to an only-ciphertext attack of DES cipher.

We will study the known-plaintext attack of DES cipher in Chapter 6 and develop the only-ciphertext attack procedure in Chapter 7.

4 Linear Approximation of S-boxes

In this section we study linear approximation of S-boxes. Similar motivation can be found in articles of Shamir [6] and Rueppel [7]. Our first approach is to investigate the probability that a value on an input bit coincides with a value on an output bit. More generally, it is useful to deal with not only one bit position but also an XORed value of several bit positions. We now start with the following definition:

Definition 1 *For given S-box S_a $(a = 1, 2, .., 8)$, $1 \leq \alpha \leq 63$ and $1 \leq \beta \leq 15$, we define $NS_a(\alpha, \beta)$ as the number of times out of 64 input patterns of S_a, such that an XORed value of the input bits masked by α coincides with an XORed value of the output bits masked by β; that is to say,*

$$NS_a(\alpha, \beta) \stackrel{\text{def}}{=} \#\{x | 0 \leq x < 64, \ (\bigoplus_{s=0}^{5}(x[s] \bullet \alpha[s])) = (\bigoplus_{t=0}^{3}(S_a(x)[t] \bullet \beta[t]))\}, \qquad (3)$$

where the symbol $\bullet$ denotes a bitwise AND operation.

Example 1

$$NS_5(16, 15) = 12. \qquad (4)$$

When $NS_a(\alpha, \beta)$ is not equal to 32, we may say that there is a correlation between the input and the output bits of S_a. For example, equation (4) indicates that the fourth input bit of S_5 coincides with an XORed value of all output bits with probability $12/64 = 0.19$. Consequently, taking account of the E expansion and the P

permutation in F-function, we see the following equation which holds with probability 0.19 for fixed K and randomly given X:

$$X[15] \oplus F(X,K)[7,18,24,29] = K[22]. \tag{5}$$

Table 1 describes part of distribution table of S-box S_5, where the vertical and the horizontal axes indicate α and β respectively, and each entry shows $NS_5(\alpha,\beta) - 32$. A complete table tells us that equation (4) is the most effective linear approximation in all S-boxes (i.e. $|NS_a(\alpha,\beta) - 32|$ is maximal); therefore, equation (5) is the best approximation of F-function.

The following Lemma is now trivial from the definition of S-boxes.

Lemma 1

(1) *$NS_a(\alpha,\beta)$ is even.*

(2) *If $\alpha = 1, 32$ or 33, then $NS_a(\alpha,\beta) = 32$ for all S_a and β.*

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	4	-2	2	-2	2	-4	0	4	0	2	-2	2	-2	0	-4
3	0	-2	6	-2	-2	4	-4	0	0	-2	6	-2	-2	4	-4
4	2	-2	0	0	2	-2	0	0	2	2	4	-4	-2	-2	0
5	2	2	-4	0	10	-6	-4	0	2	-10	0	4	-2	2	4
6	-2	-4	-6	-2	-4	2	0	0	-2	0	-2	-6	-8	2	0
7	2	0	2	-2	8	6	0	-4	6	0	-6	-2	0	-6	-4
8	0	2	6	0	0	-2	-6	-2	2	4	-12	2	6	-4	4
9	-4	6	-2	0	-4	-6	-6	6	-2	0	-4	2	-6	-8	-4
10	4	0	0	-2	-6	2	2	2	2	-2	2	4	-4	-4	0
11	4	4	4	6	2	-2	-2	-2	-2	-2	2	0	-8	-4	0
12	2	0	-2	0	2	4	10	-2	4	-2	-8	-2	4	-6	-4
13	6	0	2	0	-2	4	-10	-2	0	-2	4	-2	8	-6	0
14	-2	-2	0	-2	4	0	2	-2	0	4	2	-4	6	-2	-4
15	-2	-2	8	6	4	0	2	2	4	8	-2	8	-6	2	0
16	2	-2	0	0	-2	-6	-8	0	-2	-2	-4	0	2	10	-20
17	2	-2	0	4	2	-2	-4	4	2	2	0	-8	-6	2	4
18	-2	0	-2	2	-4	-2	-8	4	6	4	6	-2	4	-6	0
19	-6	0	2	-2	4	2	0	4	-6	4	2	-6	4	-2	0
20	4	-4	0	0	0	0	0	-4	-4	4	4	0	4	-4	0
21	4	0	-4	-4	4	-8	-8	0	0	-4	4	8	4	0	4
22	0	6	6	2	-2	4	0	4	0	6	2	2	2	0	0
23	4	-6	-2	6	-2	-4	4	4	-4	-6	2	-2	2	0	4
24	6	0	2	4	-10	-4	2	2	0	-2	0	2	4	-2	-4
25	2	4	-6	0	-2	4	-2	6	8	6	4	10	0	2	-4
26	2	2	-8	-2	4	0	2	-2	0	4	2	0	-2	-2	0
27	2	6	-4	-6	0	0	2	6	8	0	-2	-4	-6	-2	0
28	0	-2	2	4	0	-6	2	-2	6	-4	0	2	-2	0	0
29	4	-2	6	-8	0	-2	2	10	-2	-8	-8	2	2	0	4
30	-4	-8	0	-2	-2	-2	2	-2	2	-2	6	4	4	4	0
31	-4	8	-8	2	-6	-6	-2	-2	2	-2	-2	-8	0	0	-4
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 1. A distribution table of S5 (part).

5 Linear Approximation of DES Cipher

In this section we extend linear approximations of F-function to the entire algorithm. The first example is 3-round DES cipher (Figure 2). By applying equation (5) to the first round, we see the following equation which holds with probability 12/64:

$$X_2[7,18,24,29] \oplus P_H[7,18,24,29] \oplus P_L[15] = K_1[22]. \tag{6}$$

The same is true of the final round:

$$X_2[7,18,24,29] \oplus C_H[7,18,24,29] \oplus C_L[15] = K_3[22]. \tag{7}$$

Consequently, we obtain the following linear approximate expression of 3-round DES cipher by canceling common terms:

$$P_H[7,18,24,29] \oplus C_H[7,18,24,29] \oplus P_L[15] \oplus C_L[15] = K_1[22] \oplus K_3[22]. \tag{8}$$

The probability that equation (8) holds for given random plaintext P and the corresponding ciphertext C is $(12/64)^2+(1\text{-}12/64)^2=0.70$. Since equation (5) is the best linear approximation of F-function, equation (8) is the best expression of 3-round DES cipher. We can now solve equation (8) to deduce $K_1[22] \oplus K_3[22]$ using Algorithm 1. The following lemma describes the success rate of this method:

Lemma 2 *Let N be the number of given random plaintexts and p be the probability that equation (1) holds, and assume $|p-1/2|$ is sufficiently small. Then the success rate of Algorithm 1 is*

$$\int_{-2\sqrt{N}|p-1/2|}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-x^2/2}\, dx. \tag{9}$$

Table 2 shows a numerical calculation of expression (9).

N	$\frac{1}{4}\lvert p-1/2\rvert^{-2}$	$\frac{1}{2}\lvert p-1/2\rvert^{-2}$	$\lvert p-1/2\rvert^{-2}$	$2\lvert p-1/2\rvert^{-2}$
Success Rate	84.1%	92.1%	97.7%	99.8%

Table 2. The success rate of Algorithm 1.

Next, we show an example of 5-round DES cipher (Figure 3). In this case, we apply equation (5) to the second and fourth rounds, and the following linear equation (which is deduced from $NS_1(27,4) = 22$) to the first and final rounds:

$$X[27,28,30,31] \oplus F(X,K)[15] = K[42,43,45,46]. \tag{10}$$

Then an easy calculation leads to a linear approximate expression of 5-round DES cipher:

$$\begin{aligned} &P_H[15] \oplus P_L[7,18,24,27,28,29,30,31] \oplus\ C_H[15] \oplus C_L[7,18,24,27,28,29,30,31] \\ &= K_1[42,43,45,46] \oplus K_2[22] \oplus\ K_4[22] \oplus K_5[42,43,45,46]. \end{aligned} \tag{11}$$

The next lemma gives a simple method to calculate the probability that this type of equation holds:

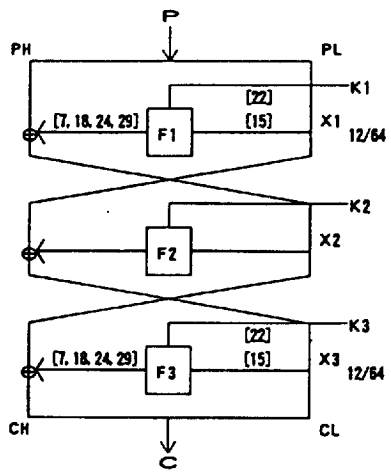
Lemma 3 *(Piling-up Lemma) Let X_i $(1 \leq i \leq n)$ be independent random variables whose values are 0 with probability p_i or 1 with probability $1-p_i$. Then the probability that $X_1 \oplus X_2 \oplus ... \oplus X_n = 0$ is*

$$1/2 + 2^{n-1} \prod_{i=1}^{n} (p_i - 1/2). \tag{12}$$

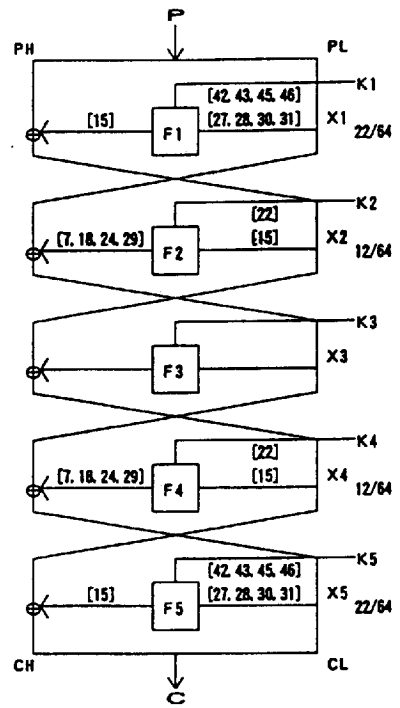
This indicates that equation (11) holds with probability $1/2+2^3(-10/64)^2(-20/64)^2 = 0.519$. Therefore, according to Lemma 2, if $|0.519 - 1/2|^{-2} = 2800$ known-plaintexts are given, one can guess the right side of the equation (11) with success rate 97.7%.

The annex shows a table of the best expression and the best probability of DES cipher up to 20 rounds. Each entry describes from left to right, the number of round, the best expression, the best probability and the linear approximation of F-function used in each round. The sign '-' represents that no approximation is needed in the round. Moreover, it should be noted that there are two best expressions in some cases, which are indicated by sign '*' in the table, because DES cipher has the round symmetry; that is, the other best expression is easily obtained by exchanging P and K_i with C and K_{N+1-i}, respectively.

It follows from this table that two key bits of 16-round DES can be deduced with high success rate using $|1.49 \times 2^{-24}|^{-2} \simeq 2^{47}$ known-plaintexts. In next chapter, we will describe a method to derive more key bits at a time.



[Fig. 2] 3-round DES cipher



[Fig. 3] 5-round DES cipher

6 Known-Plaintext Attack of DES Cipher

We are now ready for a known-plaintext attack of DES cipher. Our first example is 8-round DES cipher. As mentioned in Chapter 3, we obtain the following 8-round expression which holds with the 7-round best probability $0.5 + 1.95 \times 2^{-10}$:

$$P_H[7,18,24] \oplus P_L[12,16] \oplus C_H[15] \oplus C_L[7,18,24,29] \oplus F_8(C_L, K_8)[15] = K_1[19,23] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22]. \quad (13)$$

Although this equation contains 48-bit subkey K_8, the number of subkey bits which essentially influences $F_8(C_L, K_8)[15]$ is only six, namely, $K_8[42]$–$K_8[47]$. Therefore, we need 64 counters to carry out Algorithm 2. As regards the success rate of this method, we can prove the following lemma, which generalizes Lemma 2.

Lemma 4 *Let N be the number of given random plaintexts and p be the probability that equation (2) holds, and assume $|p - 1/2|$ is sufficiently small. Then the success rate of Algorithm 2 depends on $l_1, l_2, ..., l_d$, and $\sqrt{N}|p - 1/2|$ only.*

Generally speaking, it is not easy to calculate numerically the accurate probability above. However, under a condition it can be possible as follows.

Lemma 5 *With the same hypotheses as Lemma 4, let $q^{(i)}$ be the probability that the following equation holds for a subkey candidate $K_n^{(i)}$ and a random variable X:*

$$F_n(X, K_n)[l_1, l_2, .., l_d] = F_n(X, K_n^{(i)})[l_1, l_2, .., l_d]. \quad (14)$$

Then if $q^{(i)}$'s are independent, the success rate of Algorithm 2 is

$$\int_{x=-2\sqrt{N}|p-1/2|}^{\infty} \Big(\prod_{K_n^{(i)} \neq K_n} \int_{-x-4\sqrt{N}(p-1/2)q^{(i)}}^{x+4\sqrt{N}(p-1/2)(1-q^{(i)})} \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy \Big) \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx, \quad (15)$$

where the product is taken over all subkey candidates except K_n.

Although $q^{(i)}$'s are not independent in our situation, our experiments have shown that Lemma 5 gives a practically good approximation of the success rate, as can be seen in the following.

Now let $d = 1$ and $l_1 = 15$ in equation (2). Then a numerical calculation of expression (15) is as follows.

N	$2\|p - 1/2\|^{-2}$	$4\|p - 1/2\|^{-2}$	$8\|p - 1/2\|^{-2}$	$16\|p - 1/2\|^{-2}$
Success Rate	48.6%	78.5%	96.7%	99.9%

Table 3. The success rate of Algorithm 2 by Lemma 5 ($d = 1$, $l_1 = 15$).

Since this method can be also applied to deduction of the subkey bits of the first round, we finally obtain 14 subkey bits by carrying out Algorithm 2 twice with negligible memory. It is easy to deduce the remaining key bits, and we omit the detail. Our computer experiments indicate results better than Table 3: The program completes

deriving the whole key bits in 20 seconds using $4|1.95\times 2^{-10}|^{-2} \simeq 2^{20}$ known-plaintexts and in 40 seconds using $8|1.95 \times 2^{-10}|^{-2} \simeq 2^{21}$ known-plaintexts. The success rate of each attack is 88% and 99%, respectively.

The method to break 12-round DES cipher is almost same as 8-round DES cipher. We have succeeded in deriving the key completely in 50 hours using $8|1.91\times 2^{-16}|^{-2} \simeq 2^{33}$ known-plaintexts. Similarly, according to Lemma 4, it is possible to break 16-round DES using $8|1.19\times 2^{-22}|^{-2} \simeq 2^{47}$ known-plaintexts by solving the following expression:

$$\begin{aligned} &P_H[7,18,24] \oplus P_L[12,16] \oplus C_H[15] \oplus C_L[7,18,24,29] \oplus F_{16}(C_L, K_{16})[15] \\ &= K_1[19,23] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus K_8[44] \oplus \\ &\quad K_9[22] \oplus K_{11}[22] \oplus K_{12}[44] \oplus K_{13}[22] \oplus K_{15}[22]. \end{aligned} \tag{16}$$

Once finding 14 key bits, the remaining 42 key bits should be deduced exhaustively. Then one can break 16-round DES cipher with negligibly small memory faster than an exhaustive search for 56 key bits.

7 Only-Ciphertext Attack of DES Cipher

Now we apply Algorithm 2 to an only-ciphertext attack of DES cipher. We start with an example of 8-round DES cipher again, which has a linear approximation illustrated in Figure 4. Then we easily obtain the following expression which holds with probability $1/2 + 2^4(-2/64)(4/64)^2(-4/64)^2 = 1/2 - 2^{-17}$:

$$\begin{aligned} &P_L[27] \oplus C_H[27] \oplus C_L[0] \oplus F_8(C_L, K_8)[27] \\ &= K_2[1] \oplus K_3[8] \oplus K_4[1] \oplus K_6[1] \oplus K_7[8]. \end{aligned} \tag{17}$$

We note that $P_L[27]$ corresponds to the 39-th bit of the "real" plaintext before the initial permutation IP. Therefore, assuming that the plaintexts consist of ASCII codes, this bit must be equal to zero; that is, equation (17) has no plaintext bit. In fact, under this assumption, a similar discussion to the previous chapter tells us that seven key bits can be derived from equation (17) with high success rate using $8|2^{-17}|^{-2} = 2^{37}$ ciphertexts only.

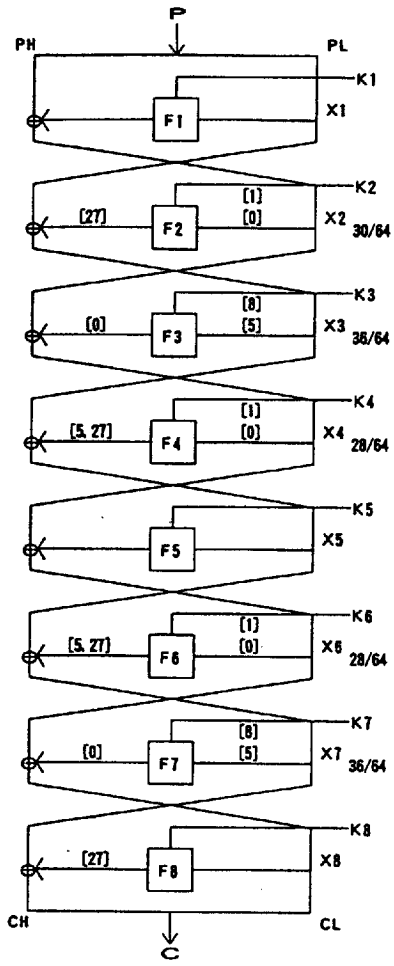
Moreover, assuming that the plaintexts consist of natural English sentences represented by ASCII codes, we can also make use of a linear approximation illustrated in Figure 5. Then we easily see the following expression which holds with probability $1/2 + 2^5(-2/64)(-6/64)(10/64)(-20/64)^3 = 1/2 - 1.83 \times 2^{-12}$:

$$\begin{aligned} &P_L[7,18,24] \oplus C_H[7,18,24,29,30] \oplus C_L[15] \oplus F_8(C_L, K_8)[30] \\ &= K_2[22] \oplus K_3[44] \oplus K_4[22] \oplus K_6[22] \oplus K_7[45] \oplus K_8[22]. \end{aligned} \tag{18}$$

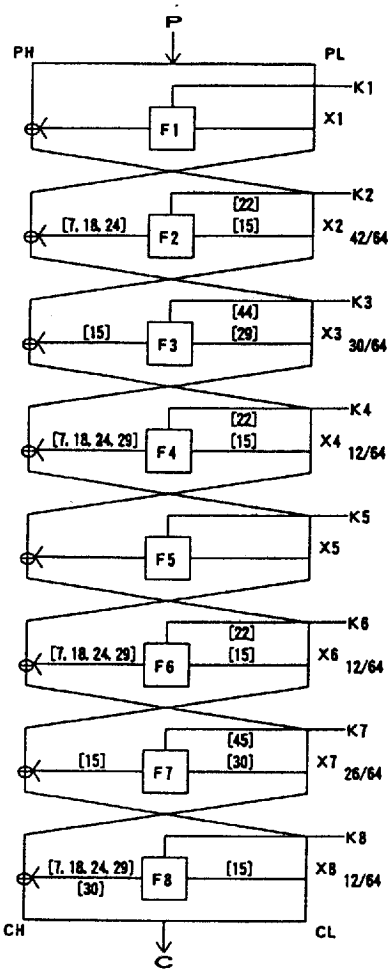
We note that $P_L[7]$,$P_L[18]$ and $P_L[24]$ correspond to the first, 45-th and 63-rd bit of the "real" plaintext, respectively. As far as we know, when the plaintexts consist of natural English sentences represented by ASCII codes, the probability of $P_L[7,18,24] = 0$ is at most 0.35. Therefore, under this assumption, the linear expression which is obtained

by eliminating $P_L[7, 18, 24]$ from equation (18) holds with probability $1/2-2\times(0.35-0.5)\times 1.83\times 2^{-12} = 1/2+1.10\times 2^{-13}$. This indicates that seven key bits can be deduced with high success rate using $8|1.10\times 2^{-13}|^{-2} \simeq 2^{29}$ ciphertexts only.

Finally, we show a situation in which 16-round DES cipher is still breakable faster than an exhaustive search for 56 bits key. We now return to equation (16), which contains five plaintext bits, and suppose that these bits are independently equal to zero with probability 80% and all other plaintext bits are random. Then the linear equation which is obtained by eliminating these five bits from equation (16) holds with probability $1/2+2^5(0.8-0.5)^5\times 1.19\times 2^{-22} = 1/2+1.48\times 2^{-26}$. This concludes that seven key bits can be obtained with high success rate using $8|1.48\times 2^{-26}|^{-2} = 1.82\times 2^{53}$ ciphertexts only.



[Fig. 4] Only-Ciphertext Attack of 8-round DES (1)



[Fig. 5] Only-Ciphertext Attack of 8-round DES (2)

8 Concluding Remarks

We have introduced a new method for cryptanalysis of DES cipher. This method has enabled us the first known-plaintext attack of the full 16-round DES cipher and the initial step toward an only-ciphertext attack. To go more deeply into the only-ciphertext attack, however, we have to deal with several problems resulting from non-randomness of plaintexts. The detail discussion of this type of attack including complete tables and proofs, which we have omitted for lack of space, will appear in the full paper.

References

[1] E.Biham and A.Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Journal of Cryptology*,Vol.4,pp.3–72,(1991).

[2] E.Biham and A.Shamir, "Differential Cryptanalysis of FEAL and N-Hash," *Advances in Cryptology - EUROCRYPT'91*, Lecture Notes in Computer Science,Vol.547, pp.1–16,(1991).

[3] E.Biham and A.Shamir, "Differential Cryptanalysis of the full 16-round DES," *CRYPTO'92 Extended Abstracts*, pp.12-1–12-5,(1992).

[4] A.Tardy-Corfdir and H.Gilbert, "A Known Plaintext Attack of FEAL-4 and FEAL-6," *Advances in Cryptology - CRYPTO'91*, Lecture Notes in Computer Science,Vol.576, pp.172–182,(1991).

[5] M.Matsui and A.Yamagishi, "A New Method for Known Plaintext Attack of FEAL Cipher," *Advances in Cryptology - EUROCRYPT'92*, Lecture Notes in Computer Science,Vol.658, pp.81–91,(1992).

[6] A.Shamir, "On the Security of DES," *Advances in Cryptology - CRYPTO'85*, Lecture Notes in Computer Science,Vol.218, pp.280–281,(1985).

[7] R.A.Rueppel, "Analysis and Design of Stream Ciphers," Springer Verlag,(1986).

3	$P_H[\alpha] \oplus P_L[15] \oplus C_H[\alpha] \oplus C_L[15]$ $= K_1[22] \oplus K_3[22]$	$1/2 + 1.56 \times 2^{-3}$	A-A
*4	$P_H[\alpha] \oplus P_L[15] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[22] \oplus K_3[22] \oplus K_4[\gamma]$	$1/2 - 1.95 \times 2^{-5}$	A-AB
5	$P_H[15] \oplus P_L[\alpha, \beta] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[\gamma] \oplus K_2[22] \oplus K_4[22] \oplus K_5[\gamma]$	$1/2 + 1.22 \times 2^{-6}$	BA-AB
*6	$P_L[\delta] \oplus C_H[\alpha] \oplus C_L[15]$ $= L_2 \oplus K_6[22]$	$1/2 - 1.95 \times 2^{-9}$	-DCA-A
*7	$P_H[\delta] \oplus P_L[12, 16] \oplus C_H[\alpha] \oplus C_L[15]$ $= K_1[19, 23] \oplus L_3 \oplus K_7[22]$	$1/2 + 1.95 \times 2^{-10}$	E-DCA-A
*8	$P_H[\delta] \oplus P_L[12, 16] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[19, 23] \oplus L_3 \oplus K_7[22] \oplus K_8[\gamma]$	$1/2 - 1.22 \times 2^{-11}$	E-DCA-AB
*9	$P_H[15] \oplus P_L[\beta, \delta] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[\gamma] \oplus K_2[22] \oplus L_4 \oplus K_8[22] \oplus K_9[\gamma]$	$1/2 - 1.91 \times 2^{-14}$	BD-DCA-AB
*10	$P_L[\alpha] \oplus C_H[\alpha] \oplus C_L[15]$ $= L_2 \oplus L_6 \oplus K_{10}[22]$	$1/2 - 1.53 \times 2^{-15}$	-ACD-DCA-A
11	$P_H[\alpha] \oplus P_L[15] \oplus C_H[\alpha] \oplus C_L[15]$ $= K_1[22] \oplus L_3 \oplus L_7 \oplus K_{11}[22]$	$1/2 + 1.91 \times 2^{-16}$	A-ACD-DCA-A
*12	$P_H[\alpha] \oplus P_L[15] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[22] \oplus L_3 \oplus L_7 \oplus K_{11}[22] \oplus K_{12}[\gamma]$	$1/2 - 1.19 \times 2^{-17}$	A-ACD-DCA-AB
13	$P_H[15] \oplus P_L[\alpha, \beta] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[\gamma] \oplus K_2[22] \oplus L_4 \oplus L_6 \oplus K_{12}[22] \oplus K_{13}[\gamma]$	$1/2 + 1.49 \times 2^{-19}$	BA-ACD-DCA-AB
*14	$P_L[\delta] \oplus C_H[\alpha] \oplus C_L[15]$ $= L_2 \oplus L_6 \oplus L_{10} \oplus K_{14}[22]$	$1/2 - 1.19 \times 2^{-21}$	-DCA-ACD-DCA-A
*15	$P_H[\delta] \oplus P_L[12, 16] \oplus C_H[\alpha] \oplus C_L[15]$ $= K_1[19, 23] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}[22]$	$1/2 + 1.19 \times 2^{-22}$	E-DCA-ACD-DCA-A
*16	$P_H[\delta] \oplus P_L[12, 16] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[19, 23] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}[22] \oplus K_{16}[\gamma]$	$1/2 - 1.49 \times 2^{-24}$	E-DCA-ACD-DCA-AB
*17	$P_H[15] \oplus P_L[\beta, \delta] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[\gamma] \oplus K_2[22] \oplus L_4 \oplus L_8 \oplus L_{12} \oplus K_{16}[22] \oplus K_{17}[\gamma]$	$1/2 - 1.16 \times 2^{-26}$	BD-DCA-ACD-DCA-AB
*18	$P_L[\alpha] \oplus C_H[\alpha] \oplus C_L[15]$ $= L_2 \oplus L_6 \oplus L_{10} \oplus L_{14} \oplus K_{18}[22]$	$1/2 - 1.86 \times 2^{-28}$	-ACD-DCA-ACD-DCA-A
19	$P_H[\alpha] \oplus P_L[15] \oplus C_H[\alpha] \oplus C_L[15]$ $= K_1[22] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus L_{15} \oplus K_{19}[22]$	$1/2 + 1.16 \times 2^{-28}$	A-ACD-DCA-ACD-DCA-A
*20	$P_H[\alpha] \oplus P_L[15] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $= K_1[22] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus L_{15} \oplus K_{19}[22] \oplus K_{20}[\gamma]$	$1/2 - 1.46 \times 2^{-30}$	A-ACD-DCA-ACD-DCA-AB

A:	$X[15] \oplus F(X, K)[7, 18, 24, 29] = K[22]$	$p = \frac{12}{64}$	α:	7,18,24,29
B:	$X[27, 28, 30, 31] \oplus F(X, K)[15] = K[42, 43, 45, 46]$	$p = \frac{22}{64}$	β:	27,28,30,31
C:	$X[29] \oplus F(X, K)[15] = K[44]$	$p = \frac{30}{64}$	γ:	42,43,45,46
D:	$X[15] \oplus F(X, K)[7, 18, 24] = K[22]$	$p = \frac{42}{64}$	δ:	7,18,24
E:	$X[12, 16] \oplus F(X, K)[7, 18, 24] = K[19, 23]$	$p = \frac{16}{64}$	L_i:	$K_i[22] \oplus K_{i+1}[44] \oplus K_{i+2}[22]$

Annex. The best expression and the best probability of DES cipher.