Linear Cryptanalysis of DES Cipher (I)

(Version 1.03)

Mitsuru Matsui

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

Abstract

This paper introduces a new methodology for cryptanalysis of block ciphers. The principle is based on a new measure of linearity and effectively applicable to Data Encryption Standard (DES). We give an explicit description of the best linear approximate expression and its approximate probability for DES and develop our analysis into the first successful known-plaintext attack faster than an exhaustive key search. As a result, DES is breakable with 2^{45} random known-plaintexts and the corresponding ciphertexts. Moreover, this method enables us to take the initial step toward a ciphertexts-only attack of block ciphers.

Key words: Data Encryption Standard, Block Cipher, Linear Cryptanalysis, Known-plaintext Attack.

1 Introduction

Data Encryption Standard (DES) [6], the first digital cipher whose structure was made public officially, is widely used as an international standard of cryptosystems for civilian applications, and generally accepted as an excellent model of a block cipher. At the same time, discussions on security of DES have been also active since the first appearance. The adequacy of the 56-bit key length, for example, has been the subject of controversy, and the secrecy of design criteria of S-boxes has provoked a great deal of public interest. Cryptanalysis of DES, especially study of S-boxes, has been a main research topic on block ciphers accordingly.

One of successful approaches to analysis of S-boxes is an observation of how changing input bits affects output bits. The first paper of cryptanalysis of DES [4] reported many remarkable characteristics of S-boxes including the fact that changing one input bit results in changing at least two output bits. Desmedt, Quisquater and Davio [3] generalized these criteria to obtain several new properties about relationship between various input changes and the corresponding output changes. To extend these local properties of S-boxes to the entire cipher structure, however, one had to wait for Differential Cryptanalysis by Biham and Shamir [1].

Differential Cryptanalysis paid attention to the probability that equation $SBOX(x \oplus \Delta x) = SBOX(x) \oplus \Delta y$ holds for randomly given x, where Δx and Δy denote fixed input and output differences, respectively. They thereby extended the local probabilistic feature of S-boxes to the entire cipher structure and gave an explicit description of statistical relations between plaintext differences and ciphertext differences. Moreover, they developed this principle into a chosen-plaintext attack, and finally showed that DES is breakable with 2^{47} chosen-plaintexts and the corresponding ciphertexts [2], which was the first successful attack faster than an exhaustive key search.

On the other hand, another noteworthy approach to analysis of S-boxes is an observation of linearity. Hellman et al. [4] and Shamir [8] pointed out strong correlation that holds between certain input bits and output bits of some S-boxes, which indicated that they are partially close to linear functions. Rueppel [7] studied linearity of S-boxes from a viewpoint of Walsh transformation of boolean functions, and showed that in some aspects S-boxes are remarkably close to linear functions. It has been unknown, however, whether such linearity of S-boxes is effective in cryptanalysis of DES.

This paper introduces a new measure of linearity of S-boxes. We concentrate our attention on the probability that equation $\bigoplus_{i \in \delta x} x[i] = \bigoplus_{j \in \delta y} SBOX(x)[j]$ holds for randomly given x, where δx and δy denote fixed subsets of input bits and output bits, respectively, and $x[i]$ is defined as the i-th bit of x. We thereby extend the local linearity of S-boxes to global linearity of the entire cipher structure, and reach non-trivial statistical linear relations between plaintext bits and ciphertext bits. The first aim of this paper is to give an explicit description of the best linear approximate expression and its approximate probability for DES.

We then carry out a known-plaintext attack of DES by regarding the linear approximate expression as a probabilistic linear equation whose unknown variables are secret key bits. As a result, we show that DES is breakable with 2^{45} random known-plaintexts and the corresponding ciphertexts, which is the first successful known-plaintext attack faster than an exhaustive key search. Our attack procedure requires no memory to preserve given plaintexts or ciphertexts.

Another important aspect of this approach is that we can derive the secret key using information on only several bit locations of plaintexts and ciphertexts, and moreover the information may be probabilistic. In other words, even if no plaintext bit is given explicitly, the attack can be successful using statistical information about the plaintexts. This observation finally leads to a ciphertexts-only attack of block ciphers. We can even show a situation in which DES is breakable by a ciphertexts-only attack faster than an exhaustive key search.

For convenience of software implementations, this paper introduces a new numbering rule to indicate bit positions, which is defined in chapter 2. All tables of DES are thereby rewritten and illustrated in annex A. Chapter 3 describes general principles of Linear Cryptanalysis in the form widely applicable to block ciphers. Chapter 4 studies linear approximation of S-boxes and chapter 5 extends the local properties of S-boxes to the entire cipher structure. Several useful approximate tables obtained here are summarized in annexes B and C. Chapter 6 applies our knowledge to a known-plaintext attack of DES and provides various experimental results, where all computer programs were implemented and executed by C and assembly language on HP9735 computer (PA-RISC 99MHz). As for a ciphertexts-only attack, which is another important consequence of Linear Cryptanalysis, we will describe the detail in the subsequent paper [5].

2 Notations and Preliminaries

Fig.1, Fig.2 Figure 1 and Figure 2 illustrate DES cipher and its F-function, respectively. Since the scope of this paper is a known-plaintext attack using random plaintexts, it is not necessary to consider the initial permutation IP and the final permutation IP^{-1}, which are one-to-one maps. We hence refer to 64-bit data after the IP as the plaintext and 64-bit data before the IP^{-1} as the ciphertext. We also call 56-bit data after the PC-1 the secret key, since the essentially secret information consists of 56 bits.

We here introduce a new numbering rule to indicate bit positions; we define the right most bit of each symbol as the zero-th bit, which is the lowest bit. Consequently, the left most bit or the highest bit of a plaintext is referred to as the 63rd, and the left most bit of a subkey is represented as the 47th. This disagrees with conventional numbering rule of DES, but is convenient for software implementations. To avoid confusion, we do not change the numbering of S-boxes. Complete tables of DES rewritten by this rule are listed in annex A.

Throughout this paper, the following notations are used unless otherwise indicated, where the suffix r that represents the round will be omitted in round-independent descriptions.

P	The 64-bit data after the IP; the plaintext.
C	The 64-bit data before the IP^{-1}; the ciphertext.
P_H	The upper 32-bit data of P.
C_H	The upper 32-bit data of C.
P_L	The lower 32-bit data of P.
C_L	The lower 32-bit data of C.
X_r	The r-th round 32-bit subdata.
K	The 56-bit data after the PC-1; the secret key.
K_r	The r-th round 48-bit subkey.
$F_r(X_r, K_r)$	The r-th round F-function.
$S_a(x)$	The a-th S-box.
$A[i]$	The i-th bit of symbol A.
$A[i, j, .., k]$	$A[i] \oplus A[j] \oplus ... \oplus A[k]$.

3 Introduction to Linear Cryptanalysis

This chapter is intended to describe general principles of Linear Cryptanalysis in the form widely applicable to various cryptosystems, and introduce an application to cryptanalytic attack of DES. The first approach to Linear Cryptanalysis is to find the following "effective" linear approximate expression which holds with probability $p \neq 1/2$ for randomly given plaintext P, the corresponding ciphertext C and fixed secret key K :

$$P[i_1, i_2, .., i_a] \oplus C[j_1, j_2, .., j_b] = K[k_1, k_2, .., k_c], \tag{1}$$

where $i_1, i_2, .., i_a, j_1, j_2, .., j_b$ and $k_1, k_2, .., k_c$ denote fixed bit locations.

Since both sides of equation (1) essentially represent one-bit information, the magnitude of $|p - 1/2|$ expresses the effectiveness. Once we succeed in reaching an effective linear approximate expression, it is possible to derive one key bit $K[k_1, k_2, .., k_c]$ from given known-plaintexts and the corresponding ciphertexts by the following simple algorithm based on 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 Algorithm 1 can be determined by N and p, and clearly increases when N or $|p - 1/2|$ does. We now refer to the most effective linear approximate expression (i.e. $|p - 1/2|$ is maximal) as the best expression and its probability as the best probability, respectively. Then our main concern is the following:

Problem 1 How to find effective linear approximate expressions.

Problem 2 An explicit description of the success rate of Algorithm 1 by N and p.

Problem 3 A search for the best expression and a calculation of the best probability.

The first aim of this paper is to solve these problems on DES. For this purpose, we begin by studying linear approximation of S-boxes in chapter 4. We introduce a new measure of linearity of S-boxes, where the resultant distribution tables, listed in annex B, will play an essential role in our story. Chapter 5 extends these local properties of S-boxes to the entire cipher structure and reaches effective linear approximate expressions of DES. In this stage, the success rate of Algorithm 1 is also discussed. As for the search problem, which has been solved by a computer program, we summarize the results in annex C.

The next aim of this paper is to give a practical method for known-plaintext attack of n-round DES. To achieve this purpose, we make use of the best expression of (n–2)-round DES; in other words, we approximate (n–2) F-functions from the second round to the (n–1)th round, while leaving the first and the final rounds unchanged. Consequently, we obtain the following type of linear approximate expression of n-round DES which contains subkeys K_1 and K_n and holds with the best probability of (n–2)-round DES:

$$P[i_1, i_2, .., i_a] \oplus C[j_1, j_2, .., j_b] \oplus F_1(P_L, K_1)[u_1, u_2, .., u_d] \oplus F_n(C_L, K_n)[v_1, v_2, .., v_e] \\ = K[k_1, k_2, .., k_c]. \qquad (2)$$

If one substitutes an incorrect subkey value for K_1 or K_n in equation (2), then the effectiveness clearly decreases. It is hence possible to derive K_1, K_n and $K[k_1, k_2, .., k_c]$ from given known-plaintexts and the corresponding ciphertexts by the following algorithm based on maximum likelihood method, which generalizes Algorithm 1:

Algorithm 2

Step1 Let ${K_1}^{(i)}$ ($i = 1, 2, ...$) and ${K_n}^{(j)}$ ($j = 1, 2, ...$) be possible candidates for K_1 and K_n, respectively. Then for each pair $({K_1}^{(i)}, {K_n}^{(j)})$, let $T_{i,j}$ 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 $T_{i,j}$'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 and the computational complexity of Algorithm 2 will be discussed in chapter 6. We have implemented this method with computer software and succeeded in experimentally breaking DES up to 12 rounds. These results and further application to the full 16-round DES are also described in the same chapter.

It should be noted that Linear Cryptanalysis is also applicable to a ciphertexts-only attack. Consider, for example, the case where we approximate (n–1) F-functions from the first round to the (n–1)th round, while the last round unchanged. We then obtain the following linear approximate expression of n-round DES which holds with the best probability of (n–1)-round DES:

$$P[i_1, i_2, .., i_a] \oplus C[j_1, j_2, .., j_b] \oplus F_n(C_L, K_n)[v_1, v_2, .., v_e] = K[k_1, k_2, .., k_c]. \qquad (3)$$

Now assuming that the probability of $P[i_1, i_2, .., i_a] = 0$ is not equal to 1/2, then even if we eliminate the term $P[i_1, i_2, .., i_a]$ from equation (3), the resultant expression may be still effective. This suggests that K_n and $K[k_1, k_2, .., k_c]$ can be derived from only statistical information about the plaintexts. The detailed discussion of this type of attack will appear in the subsequent paper [5].

4 Linear Approximation of S-boxes

Our first approach to linear approximation of S-boxes is to investigate correlation between an input bit and an output bit for random input values. It is easily seen, for example, that the third input bit of the third S-box agrees with the first output bit 38 times out of 64 input patterns, which indicates that equation $S_3(x)[1] = x[3]$ holds with probability $38/64 = 0.59$ for randomly given x. More generally, it is useful to treat not only one bit position but also an XORed value of several bit positions. This leads to a new measure of linearity of S-boxes as follows:

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 agrees with an XORed value of the output bits masked by β; that is to say,*

$$NS_a(\alpha, \beta) \stackrel{\text{def}}{=} \#\{x | 0 \leq x < 64, \quad (\bigoplus_{s=0}^{5}(x[s] \bullet \alpha[s])) = \ (\bigoplus_{t=0}^{3}(S_a(x)[t] \bullet \beta[t]))\}, \tag{4}$$

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

Example 1 (Shamir [6])

$$NS_5(16, 15) = 12. \tag{5}$$

When $NS_a(\alpha, \beta)$ is not equal to 32, we may say that there is a correlation between input bits and output bits of S_a, and magnitude of $|NS_a(\alpha, \beta) - 32|$ represents the effectiveness. Equation (5) tells us that the fourth input bit of S_5 agrees 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:

$$X[15] \oplus F(X, K)[7, 18, 24, 29] = K[22]. \tag{6}$$

Equivalently, the following equation holds with probability $1 - 0.19 = 0.81$.

$$X[15] \oplus F(X, K)[7, 18, 24, 29] = K[22] \oplus 1. \tag{7}$$

Fig.3 The situation above is illustrated as Figure 3. A similar illustration will be employed in the rest of this paper. Annex B shows complete distribution tables of S-boxes, where the vertical and the horizontal axes indicate α and β, respectively, and each entry denotes $NS_a(\alpha, \beta) - 32$. Note that since equation (5) is the most effective linear approximation of all S-boxes (i.e. $|NS_a(\alpha, \beta) - 32|$ is maximal), equation (6) or (7) is the best linear 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.*

5 Linear Approximation of DES Cipher

This chapter provides several examples to show how to extend linear approximations of F-function obtained in the preceding chapter to the entire cipher structure of DES. We will see that Piling-up Lemma (Lemma 3) is a key formula which connects local approximate probability with global approximate probability. We also describe the best expression and the best probability of DES found by a computer search.

5.1 3-round DES

Fig.4 The first example is 3-round DES (Figure 4). By applying equation (6) to the first round, we have the following equation which holds with probability 12/64:

$$X_2[7,18,24,29] \oplus P_H[7,18,24,29] \oplus P_L[15] = K_1[22]. \tag{8}$$

The same is true of the final round:

$$X_2[7,18,24,29] \oplus C_H[7,18,24,29] \oplus C_L[15] = K_3[22]. \tag{9}$$

Consequently, we obtain the following linear approximate expression of 3-round DES without any intermediate value by canceling the common term X_2:

$$P_H[7,18,24,29] \oplus C_H[7,18,24,29] \oplus P_L[15] \oplus C_L[15] = K_1[22] \oplus K_3[22]. \tag{10}$$

Equation (10) holds if and only if both of equations (8) and (9) hold, or neither of them hold; hence the probability is $(12/64)^2 + (1-12/64)^2 = 0.70$ for random known-plaintext P and the corresponding ciphertext C. Since equation (6) is the best linear approximation of F-function, equation (10) is the best expression of 3-round DES. We can now apply Algorithm 1 to equation (10) and derive $K_1[22] \oplus K_3[22]$. The success rate of Algorithm 1 is shown by the following lemma, whose proof is easily given by approximating binary distribution with normal distribution:

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

$$\int_{-2\sqrt{N}|p-1/2|}^{\infty} \frac{1}{\sqrt{2\pi}}\, e^{-x^2/2}\, dx. \tag{11}$$

Corollary 1 *With the same assumption as Lemma 2, the success rate of Algorithm 1 depends on $\sqrt{N}|p-1/2|$ only.*

Table 1 shows a numerical calculation of expression (11).

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

Table 1. The success rate of Algorithm 1.

5.2 5-round DES

Fig.5 The next example is 5-round DES (Figure 5). In this case, we apply equation (6) to the second round, and the following equation, derived from $NS_1(27,4) = 22$, to the first round:

$$X[27,28,30,31] \oplus F(X,K)[15] = K[42,43,45,46]. \tag{12}$$

Then we have the following equation which holds with probability $(12/64)(22/64) + (1-12/64)(1-22/64) = 0.598$:

$$\begin{aligned} &X_3[7,18,24,29] \oplus P_H[15] \oplus P_L[7,18,24,27,28,29,30,31] \\ &= K_1[42,43,45,46] \oplus K_2[22]. \end{aligned} \tag{13}$$

The same is true of the fourth and the final rounds:

$$\begin{aligned} &X_3[7,18,24,29] \oplus C_H[15] \oplus C_L[7,18,24,27,28,29,30,31] \\ &= K_4[22] \oplus K_5[42,43,45,46]. \end{aligned} \tag{14}$$

Consequently, we see the following linear approximate expression of 5-round DES without any intermediate value by canceling the common term X_3:

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

The probability that equation (15) holds is $0.598^2+(1-0.598)^2 = 0.519$. According to Lemma 2, if $|0.519 - 1/2|^{-2} = 2750$ random known-plaintexts and the corresponding ciphertexts are available, one can guess the right side of the equation (15) with the success rate 97.7%. We will later see that this equation is the best expression of 5-round DES.

In the rest of this paper, we will establish various linear approximate expressions of the entire cipher structure by piling up linearized F-functions round by round. The following lemma gives a handy method to calculate global approximate probability of the entire cipher using local approximate probability of S-boxes or F-functions. The proof is easily given by induction on n:

Lemma 3 (Piling-up Lemma) *Let X_i $(1 \le i \le n)$ 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*

$$1/2 + 2^{n-1}\prod_{i=1}^{n}(p_i - 1/2). \tag{16}$$

Example 2 *The probability that equation (15) holds can be also calculated as*

$$1/2 + 2^3(12/64 - 1/2)^2(22/64 - 1/2)^2 = 0.519. \tag{17}$$

5.3 Extension to arbitrary round DES

To establish linear approximate expressions of arbitrary round DES, we start with
Fig.6 the following 5-round approximation (Figure 6):

$$X_1[7,18,24,29] \oplus X_5[7,18,24] \ = K_2[22] \oplus K_3[44] \oplus K_4[22], \tag{18}$$

which can be obtained by applying (6) to the second round, and the following two equations, derived from $NS_1(4,4) = 30$ and $NS_5(16,14) = 42$, to the third and the fourth rounds, respectively:

$$X[29] \oplus F(X,K)[15] = K[44], \tag{19}$$

$$X[15] \oplus F(X,K)[7,18,24] = K[22]. \tag{20}$$

According to Piling-up Lemma, equation (18) holds with probability $1/2+2^2(-20/64)(-2/64)(10/64) = 0.506$. Although this probability is worse than that of the preceding 5-round approximation, equation (18) contains X_1 and X_5 only, and hence we can use this relation repeatedly to reach linear approximate expressions of arbitrary round
Fig.7 DES. We now show an example of 16-round DES (Figure 7), where we approximate each round as follows:

The first round:	equation (21),
The 3rd, 4th and 5th rounds:	equation (18),
The 7th, 8th and 9th rounds:	equation (18),
The 11th, 12th and 13th rounds:	equation (18),
The 15th round:	equation (6).
The 16th round:	equation (12).

Equation (21) is derived from $NS_5(34,14) = 16$ as follows:

$$X[7,18,24] \oplus F(X,K)[12,16] = K[19,23]. \tag{21}$$

As a result, we obtain the following linear approximate expression of 16-round DES without any intermediate value:

$$\begin{aligned} &P_H[7,18,24] \oplus P_L[12,16] \oplus C_H[15] \oplus \ C_L[7,18,24,27,28,29,30,31] \\ &= K_1[19,23] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus \ K_7[22] \oplus K_8[44] \oplus K_9[22] \oplus \\ &\quad K_{11}[22] \oplus K_{12}[44] \oplus K_{13}[22] \oplus \ K_{15}[22] \oplus K_{16}[42,43,45,46]. \end{aligned} \tag{22}$$

According to Piling-up Lemma again, equation (22) holds with probability $1/2 + 2^{11}(-20/64)^4(-10/64)(-2/64)^3(10/64)^3(-16/64) = \ 1/2 - 1.49 \times 2^{-24}$ for random known-plaintexts and the corresponding ciphertexts. Lemma 2 tells us that the right side of equation (22) can be derived with the success rate 97.7% when $(1.49\times2^{-24})^{-2} = 1.80 \times 2^{46}$ known-plaintexts are available.

5.4 The best expression and the best probability of DES

We can prove that the linear approximate expressions illustrated in Figures 4, 5 and 7 give the best expressions of each round-reduced DES. Annex C summarizes a complete table of the best expression and the best probability of DES up to 20 rounds, where 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 '-' shows that no approximation is needed in the round. It should be noted that there are two best expressions in some cases, which are indicated by sign '$*$' in the table, because DES has "round symmetry"; in other words, the other best expression is easily obtained by exchanging P and C and also exchanging K_i and K_{n+1-i}. The results in annex C have been obtained by a computer search, where the program consists of 350 lines with C language and has completed the search within a minute. We remark that all entries in annex C are established by approximating at most one S-box in each round as a result, but for the complete search, we have to take into consideration the case where two or more S-boxes are approximated in a single round.

According to annex C, 16-round DES has two best equations, each of which holds with probability $1/2 - 1.49 \times 2^{-24}$. We can hence derive two subkey bits with the success rate $(97.7)^2 = 95\%$ using $|1.49 \times 2^{-24}|^{-2} = 1.80 \times 2^{46}$ random known-plaintexts and the corresponding ciphertexts. In the next chapter, we will present more effective method to obtain more key bits at a time.

We close this chapter with showing an interesting property of F-function which can appear when we approximate two S-boxes in a single round. Consider the following two linear approximations of F-function:

$$X[3,4] \oplus F(X,K)[0,10,20,25] = K[6,7], \tag{23}$$

$$X[3,4] \oplus F(X,K)[5,11,27] = K[4,5]. \tag{24}$$

These equations are derived from $NS_7(3,15) = 40$ and $NS_8(48,13) = 20$, respectively, and hence we have the following equation which holds with probability $1/2 + 2(8/64)(-12/64) = 0.453$ by canceling the common term X:

$$F(X,K)[0,5,10,11,20,25,27] = K[4,5,6,7], \tag{25}$$

The left side of equation (25) does not contain any input information on F-function. In other words, assuming that input data X is random, we can derive one key bit $K[4,5,6,7]$ from only output information without any input information. According to Lemma 2, the success rate of this derivation is 97.7%, if one has $(0.5 - 0.453)^{-2} = 460$ output texts. There are essentially eight relations of this type, of which equation (25) attains the best probability. We can establish linear approximate expressions
Fig.8 of arbitrary round DES by piling up equation (25) in every other round (Figure 8), though the resultant global probability is worse than that of annex C. It is also possible to show a known-plaintext attack of 16-round DES faster than an exhaustive key search using this expression, and we summarize the detail in annex D.

6 Known-Plaintext Attack of DES Cipher

We are now ready to apply our knowledge to known-plaintext attack of DES cipher. This chapter makes a detailed description of a practical method to derive the whole of the secret key bits from random known-plaintexts and the corresponding ciphertexts. We show various results of computer experiments to break reduced DES up to twelve rounds, where an implementation of Algorithm 2 will play an essential role in our attack. Another purpose of this chapter is to establish global theory of Linear Cryptanalysis; we prove a key lemma (Lemma 4), which enables us to predict the attack success rate of larger round DES using experimental results of smaller round DES. As a result, we will finally reach a known-plaintext attack of the full 16-round DES faster than an exhaustive key search.

6.1 8-round DES

The first example is 8-round DES. As mentioned in Chapter 3, we begin by describing 8-round DES using the 6-round best expression; that is to say, we approximate six F-functions from the second round to the seventh round, while leaving the first and the final rounds unchanged (Figure 9). Consequently, we obtain the following expression of 8-round DES which holds with the 6-round best probability $1/2 + 1.95 \times 2^{-10}$ for random known-plaintexts and the corresponding ciphertexts (see annex C for detail):

Fig.9

$$P_H[7,18,24] \oplus F_1(P_L,K_1)[7,18,24] \oplus C_H[15] \oplus C_L[7,18,24,29] \oplus F_8(C_L,K_8)[15]$$
$$= K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22]. \tag{26}$$

Our purpose is to solve equation (26) using Algorithm 2 and derive some of the subkey bits. Let us now consider how many text bits and subkey bits are required to calculate the left side of equation (26). A careful observation tells us that the following 25 bits essentially affect the left side:

- (Known) text information (13 bits): $P_L[11] \sim P_L[16]$, $C_L[0]$, $C_L[27] \sim C_L[31]$, $P_H[7,18,24] \oplus C_H[15] \oplus C_L[7,18,24,29]$,
- (Unknown) subkey information (12 bits): $K_1[18] \sim K_1[23]$, $K_8[42] \sim K_8[47]$.

It should be noticed that the term $P_H[7,18,24] \oplus C_H[15] \oplus C_L[7,18,24,29]$ represents one-bit information. We refer to these known 13 bits and unknown 12 bits as the effective text bits and the effective key bits of equation (26), respectively. Under this terminology, we can generally say that Algorithm 2 is a method to derive the effective key bits and the right side of equation (2) from information on the effective text bits. Note again that we do not need any text information outside the effective text bits.

There are several possible ways to realize Algorithm 2. We here present a practical implementation which does not require any memory to preserve given plaintexts or ciphertexts. In the following story, we first count text frequency on the effective text bits and then count key frequency on the effective key bits.

Algorithm 2-A

[Data Counting Phase]

Step 1 Prepare 2^{13} counters U_i $(0 \leq i < 2^{13})$ and initialize them by zeros, where i corresponds to each value on the 13 effective text bits of equation (26).

Step 2 For each plaintext P and the corresponding ciphertext C, compute the value 'i' of **Step 1** and count up the counter U_i by one.

[Key Counting Phase]

Step 3 Prepare 2^{12} counters T_j $(0 \leq j < 2^{12})$ and initialize them by zeros, where j corresponds to each value on the 12 effective key bits of equation (26).

Step 4 For each 'j' of **Step 3**, let T_j be the sum of U_i's such that the left side of (26), whose value can be uniquely determined by i and j, is equal to zero.

Step 5 Let T_{max} be the maximal value and T_{min} be the minimal value of all T_j's.

- If $|T_{max} - N/2| > |T_{min} - N/2|$, then adopt the subkey value 'j' corresponding to T_{max} and guess that the right side of equation (26) is 0.
- If $|T_{max} - N/2| < |T_{min} - N/2|$, then adopt the subkey value 'j' corresponding to T_{min} and guess that the right side of equation (26) is 1.

In general, the computational complexity of this method is $O(N) + O(2^{t+k})$, where t and k denote the number of the effective text bits and the number of the effective key bits, respectively. The size of counters to be required is $2^t + 2^k = 1.5 \times 2^{13}$.

We have implemented Algorithm 2-A with computer software, which is described by C and assembly languages. Our program solves equation (26) while generating random plaintexts and enciphering them. The experimental results on the success rate and the computing time are as follows, where each entry shows an average value of 1000 trials:

N	2^{18}	2^{19}	2^{20}
Success Rate	49.4%	93.2%	100%
Running Time	2.4sec	3.0sec	4.2sec

Table 2. The results of our experiments to solve equation (26).

This makes 13 subkey bits. To derive more subkey bits, we make use of "round symmetry" of DES; that is to say, we obtain another expression of 8-round DES which holds with the same probability as equation (26) by exchanging P and C and also exchanging K_i with K_{9-i}.

$$C_H[7,18,24] \oplus F_8(C_L,K_8)[7,18,24] \oplus P_H[15] \oplus P_L[7,18,24,29] \oplus F_1(P_L,K_1)[15]$$
$$= K_6[22] \oplus K_5[44] \oplus K_4[22] \oplus K_2[22]. \quad (27)$$

The solution of this equation gives us $K_1[42] \sim K_1[47]$, $K_8[18] \sim K_8[23]$ and one subkey bit of the right side of equation (27). Note that we can carry out the two procedures to solve equations (26) and (27) at the same time. In this stage, we have 26 subkey bits, which correspond to the following 23 secret key bits, since three subkey bits are duplicate according to the key-scheduling structure:

$$0, 1, 3, 5, 8, 11, 14, 15, 18, 20, 23, 24, 28, 31, 37,$$
$$38, 41, 44, 46, 50, 53, 54,\ \ 2 \oplus 22 \oplus 26 \oplus 52.$$

The remaining $56 - 23 = 33$ secret key bits are now easily obtained by an exhaustive search. Our computer program, which occupies 400KB memory in running, realizes the story above to derive the whole of the 56 secret key bits from random known-plaintexts and the corresponding ciphertexts. The results of our experiments are as follows, where the second row denotes the computing time to derive the first 23 secret key bits, and the third row indicates the total running time including an exhaustive search for the remaining 33 secret key bits:

N	2^{18}	2^{19}	2^{20}
Success Rate	25.4%	86.5%	99.9%
Running Time (1)	4.3sec	5.0sec	6.4sec
Running Time (2)	300min	300min	300min

Table 3. The results of our experiments to break 8-round DES.

Next, we show an alternative implementation of Algorithm 2 to break 8-round DES. The purpose of this approach is to reduce the computing time in return for increase of the number of plaintexts to be required. We begin with the following linear approximate expression of 6-round DES:

$$\begin{aligned} & P_L[7, 18, 24, 29] \oplus C_H[7, 18, 24] \oplus C_L[12, 16] \\ & = K_2[22] \oplus K_3[44] \oplus K_4[22] \oplus K_6[19, 23]. \end{aligned} \tag{28}$$

This equation is derived from the form "`-ACD-E`" (see notations in annex C), and holds with probability $1/2 + 2^3(-20/64)(-2/64)(10/64)(-16/64) = 1/2 - 1.56 \times 2^{-9}$. Our search program, described in Chapter 5, has found that equation (28) is the second best expression of 6-round DES. We hence obtain the following expression of 8-round DES by applying equation (28) form the second round to the seventh round,
Fig.10 while leaving the first and the final rounds unchanged (Figure 10):

$$\begin{aligned} & P_H[7, 18, 24, 29] \oplus F_1(P_L, K_1)[7, 18, 24, 29] \oplus C_H[12, 16] \oplus\ C_L[7, 18, 24] \oplus \\ & \quad F_8(C_L, K_8)[12, 16] \\ & = K_3[22] \oplus K_4[44] \oplus\ K_5[22] \oplus K_7[19, 23]. \end{aligned} \tag{29}$$

Let us now consider how many text bits and subkey bits essentially affect the left side of equation (29). We easily see that equation (29) has 17 effective text bits and 18 effective key bits as follows:

- Effective text bits (17 bits): $P_L[11] \sim P_L[16]$, $C_L[15] \sim C_L[24]$,
$P_H[7,18,24,29] \oplus C_H[12,16] \oplus C_L[7,18,24]$,
- Effective key bits (18 bits): $K_1[18] \sim K_1[23]$, $K_8[24] \sim K_8[35]$.

Although it is possible to derive 19 subkey bits with $2^{17} + 2^{18} = 1.5 \times 2^{18}$ counters by the same method as Algorithm 2-A, the complexity of **Step 4** would be too large. We hence provide an alternative approach as follows, which solves equations (26) and (29) at a time and reduces the computational complexity:

Algorithm 2-B

[Data Counting Phase 1]

Step 1 Prepare 2^{13} counters U_i $(0 \leq i < 2^{13})$ and 2^{17} counters V_j $(0 \leq j < 2^{17})$, and initialize them by zeros, where i and j correspond to each value on the 13 effective text bits of equation (26) and the 17 effective key bits of equation (29), respectively.

Step 2 For each plaintext P and the corresponding ciphertext C, compute 'i' and 'j' of **Step 1**, and count up the counters U_i and V_j by one.

[Key Counting Phase 1]

Step 3 Solve equation (26) using U_i's. We then have the 12 effective key bits and one subkey bit of the right side of equation (26).

In this stage, we are able to calculate the exact value of $F_1(P_L, K_1)$. It is hence possible to regard the effective text bits and the effective key bits of equation (29) essentially as follows:

- Effective text bits (11 bits): $C_L[15] \sim C_L[24]$,
$F_1(P_L, K_1)[7,18,24,29] \oplus P_H[7,18,24,29]$
$\oplus C_H[12,16] \oplus C_L[7,18,24]$,
- Effective key bits (12 bits): $K_8[24] \sim K_8[35]$.

This enables us to "pack" V_j's into the following new counters W_k:

[Data Counting Phase 2]

Step 4 Prepare 2^{11} counters W_k $(0 \leq k < 2^{11})$ and initialize them by zeros, where k corresponds to each value on the 11 effective text bits above.

Step 5 For each 'j' $(0 \leq j < 2^{17})$, compute 'k' of **Step 4**, whose value is uniquely determined by j, and add V_j to W_k.

[Key Counting Phase 2]

Step 6 Solve equation (29) using W_k's. We then have the 12 effective key bits above and the right side of equation (29).

We now have 26 subkey bits in all. Next, according to round symmetry of DES again, we obtain another second best expression of 8-round DES, which enables us to derive 26 more subkey bits:

$$
\begin{aligned}
& C_H[7,18,24,29] \oplus F_8(C_L,K_8)[7,18,24,29] \oplus P_H[12,16] \ \oplus P_L[7,18,24] \oplus \\
& \quad F_1(P_L,K_1)[12,16] \\
& = K_6[22] \oplus K_5[44] \oplus K_4[22] \oplus K_2[19,23]. \qquad (30)
\end{aligned}
$$

Note that we can carry out the two procedures to solve equations (29) and (30) at the same time. In this stage, we have 52 subkey bits, which correspond to the following 38 secret key bits, since 14 subkey bits are duplicate according to the key-scheduling structure:

$$
\begin{gathered}
0,1,3,5,8,11,14,15,18,20,23,24,25,28,29,30,31 \\
32,34,35,36,37,38,39,40,41,42,43,44,46,47, \\
48,50,51,53,54, \ \ 2\oplus 7\oplus 13, \ \ 2\oplus 22\oplus 26\oplus 52.
\end{gathered}
$$

The remaining $56-38=18$ secret key bits are now easily obtained by an exhaustive search. Our computer program, which occupies 1MB memory in running, realizes the story above to derive the whole of 56 secret key bits from random known-plaintexts and the corresponding ciphertexts. The results of our experiments are as follows, where the second row denotes the computing time to derive the first 38 secret key bits, and the third row indicates the total running time including an exhaustive search for the remaining 18 secret key bits. Each entry shows an average value of 1000 trials:

N	2^{18}	2^{19}	2^{20}
Success Rate	8.7%	63.0%	96.2%
Running Time (1)	5.1sec	6.4sec	8.6sec
Running Time (2)	6.3sec	7.6sec	9.8sec

Table 4. Another results of our experiments to break 8-round DES.

6.2 12-round DES

Our next example is 12-round DES. The main procedure to break 12-round DES is the same as the case of 8-round DES. We begin by describing 12-round DES using 10-round best expression; that is to say, we approximate ten F-functions from the second round to the the eleventh round, while leaving the first and the final rounds
Fig.11 unchanged (Figure 11). Consequently, we obtain the following expression of 12-round DES which holds with the 10-round best probability $1/2 - 1.53\times 2^{-15}$ for random known-plaintexts and the corresponding ciphertexts (see annex C for detail):

$$
\begin{aligned}
& P_H[7,18,24,29] \oplus F_1(P_L,K_1)[7,18,24,29] \oplus C_H[15] \ \oplus C_L[7,18,24,29] \oplus \\
& \quad F_{12}(C_L,K_{12})[15] \\
& = K_3[22] \oplus K_4[44] \oplus \ K_5[22] \oplus K_7[22] \oplus K_8[44] \oplus K_9[22] \oplus K_{11}[22]. \qquad (31)
\end{aligned}
$$

The effective text bits and the effective key bits of equation (31) are as follows:

- Effective text bits (13 bits): $P_L[11] \sim P_L[16],\ C_L[0],\ C_L[27] \sim C_L[31],$
  $P_H[7,18,24,29] \oplus C_H[15] \oplus C_L[7,18,24,29],$
- Effective key bits (12 bits): $K_1[18] \sim K_1[23],\ K_{12}[42] \sim K_{12}[47].$

We can thus derive the 12 effective key bits and one subkey bit of the right side of equation (31) with $2^{13} + 2^{12} = 1.5 \times 2^{13}$ counters. We have implemented Algorithm 2 with computer software, which program yielded the following results on the success rate and the computing time, where each entry shows an average value of 100 trials:

N	2^{30}	2^{31}	2^{32}
Success Rate	17%	55%	97%
Running Time	56min	112min	224min

Table 5. The results of our experiments to solve equation (31).

Next, according to round symmetry of DES, we have another expression of 12-round DES which holds with the same probability as equation (31):

$$\begin{aligned} & C_H[7,18,24,29] \oplus F_{12}(C_L, K_{12})[7,18,24,29] \oplus \ P_H[15] \oplus P_L[7,18,24,29] \oplus \\ & \quad F_1(P_L, K_1)[15] \\ & = K_{10}[22] \oplus K_9[44] \oplus \ K_8[22] \oplus K_6[22] \oplus K_5[44] \oplus K_4[22] \oplus K_2[22]. \end{aligned} \tag{32}$$

The solution of this equation gives us $K_1[42] \sim K_1[47]$, $K_{12}[18] \sim K_{12}[23]$ and one subkey bit of the right side of equation (32). Note that we can carry out the two procedures to solve equations (31) and (32) at the same time. In this stage, we have 26 subkey bits, which correspond to the following 25 secret key bits, since one subkey bit is duplicate according to the key-scheduling structure:

$$\begin{gathered} 0,3,4,8,11,14,16,18,22,24,26,30,31,34,38,39, \\ 41,44,46,49,50,52,54,\ \ 2 \oplus 15 \oplus 45,\ \ 13 \oplus 17 \oplus 20. \end{gathered}$$

The remaining $56 - 25 = 31$ key bits are now easily obtained by an exhaustive search. Our computer program, which occupies 400KB memory in running, derives the whole of the 56 secret key bits from random known-plaintexts and the corresponding ciphertexts. The result of our experiments are as follows, where the notations are the same as Tables 3 and 4.

N	2^{30}	2^{31}	2^{32}
Success Rate	5%	31%	94%
Running Time (1)	63min	125min	250min
Running Time (2)	169min	225min	337min

Table 6. The results of our experiments to break 12-round DES.

6.3 16-round DES

The final section of this chapter treats 16-round DES. The main story to break 16-round DES is the same as the case of 8-round or 12-round DES. As usual, we begin by describing 16-round DES using the 14-round best expression; we approximate fourteen F-functions from the second round to the fifteenth round, while leaving the first round and the final round unchanged (Figure 12). Consequently, we have the following expression of 16-round DES which holds with the 14-round best probability $1/2 - 1.19 \times 2^{-21}$ for random known-plaintexts and the corresponding ciphertexts:

Fig.12

$$\begin{aligned} &P_H[7,18,24] \oplus F_1(P_L, K_1)[7,18,24] \oplus C_H[15] \oplus C_L[7,18,24,29] \oplus F_{16}(C_L, K_{16})[15] \\ &= K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus K_8[44] \oplus K_9[22] \oplus K_{11}[22] \oplus K_{12}[44] \oplus \\ &\quad K_{13}[22] \oplus K_{15}[22]. \end{aligned} \tag{33}$$

The effective text bits and the effective key bits of equation (33) are as follows:

- Effective text bits (13 bits): $P_L[11] \sim P_L[16]$, $C_L[0]$, $C_L[27] \sim C_L[31]$, $P_H[7,18,24] \oplus C_H[15] \oplus C_L[7,18,24,29]$,
- Effective key bits (12 bits): $K_1[18] \sim K_1[23]$, $K_{16}[42] \sim K_{16}[47]$.

Applying Algorithm 2 to equation (33) with $2^{13} + 2^{12} = 1.5 \times 2^{13}$ counters, we obtain the 12 effective key bits and one subkey bit of the right side of equation (33), but the computer experiment is no longer practical in respect of the computational complexity. Then our next purpose is to estimate the number of plaintexts to be required for the successful attack. The remaining part of this chapter is assigned to give a solution of this problem.

We now consider Lemma 2 again, whose corollary says that the success rate of Algorithm 1 depends on the magnitude of $\sqrt{N}|p - 1/2|$ only. This motivates us to investigate whether similar statement holds for Algorithm 2. To do this, we have made computer experiments to compare the efficiency of our attack of 8-round DES with that of 12-round DES. The following table shows the probability that equations (26) and (31) are solvable with $N = a|p - 1/2|^{-2}$ $(a = 2, 4, 8)$ plaintexts, where p denotes the 6-round best probability $1/2 - 1.95 \times 2^{-9}$ or the 10-round best probability $1/2 - 1.53 \times 2^{-15}$ according as equation (26) or (31):

N	$2\|p - 1/2\|^{-2}$	$4\|p - 1/2\|^{-2}$	$8\|p - 1/2\|^{-2}$
Equation (26)	$N = 1.05 \times 2^{17}$	$N = 1.05 \times 2^{18}$	$N = 1.05 \times 2^{19}$
	17.9%	53.7%	94.8%
Equation (31)	$N = 1.72 \times 2^{29}$	$N = 1.72 \times 2^{30}$	$N = 1.72 \times 2^{31}$
	13%	46%	91%

Table 7. The results of our experiments to solve equations (26) and (31).

It is hence expected that equation (33) is also solvable with high success probability when $8|1.19 \times 2^{-21}|^{-2} = 1.41 \times 2^{44}$ known-plaintexts are available. In fact, we can generalize Lemma 2 in the following form:

Lemma 4 *Let N be the number of given random plaintexts and p be the probability that equation (2) holds. Assuming that $|p-1/2|$ is sufficiently small, the success rate of Algorithm 2 depends on $u_1, u_2, ..., u_d,\ v_1, v_2, ..., v_e$, and $\sqrt{N}|p-1/2|$ only.*

Proof. We may assume $p > 1/2$ and $K[k_1, k_2, .., k_c] = 0$ without loss of generality. Throughout this proof, we use the terms "the effective text bits" and "the effective key bits" to refer to the text bits and the key bits which affect $F_1(P_L, K_1)[u_1, u_2, ..., u_d] \oplus F_n(C_L, K_n)[v_1, v_2, ..., v_e]$. We then define the number of the effective text bits and the effective key bits as t and k, respectively. Our goal is to give an explicit description of the success rate of Algorithm 2. To realize this, we start with several preparations.

Firstly, we define possible events E_i and $\overline{E}_i$ $(0 \le i < 2^t)$ for a pair of a plaintext P and the corresponding ciphertext C as follows:

E_i: The case where the value on the effective text bits is equal to i, and the left side of equation (2) is equal to zero.

$\overline{E}_i$: The case where the value on the effective text bits is equal to i, and the left side of equation (2) is equal to one.

We remark that E_i's and $\overline{E}_i$'s are exclusive events, and every pair of P and C belongs to one of E_i's or $\overline{E}_i$'s. The probability that E_i and $\overline{E}_i$ take place is represented by p_i and $\overline{p}_i$, respectively, where we may suppose that $p_i = p/2^t$ and $\overline{p}_i = (1-p)/2^t$.

Next, we define a set B as $\{\ i \mid 0 \le i < 2^t\ \}$, and introduce a subset B_j of B for each j $(0 \le j < 2^k)$ as follows:

$$\begin{aligned} B_j \stackrel{\text{def}}{=} \{\ i \mid 0 \le i < 2^t,\quad & F_1(i_1, K_1)[u_1, u_2, .., u_d]\ \oplus F_n(i_n, K_n)[v_1, v_2, .., v_e] \\ & = F_1(i_1, j_1)[u_1, u_2, .., u_d]\ \oplus F_n(i_n, j_n)[v_1, v_2, .., v_e]\ \}, \end{aligned} \tag{34}$$

where each 'j' corresponds to the value on the effective key bits, and i_1 and i_n indicate F_1 and F_n components of i, respectively. The same applies to j_1 and j_n. Note that if j agrees with the correct key value j', then $B_{j'} = B$.

We are now ready to make a description of the success rate of Algorithm 2. When we apply Algorithm 2 to equation (2) with N known-plaintexts, let a_i and $\overline{a}_i$ be the number of texts which belong to E_i and $\overline{E}_i$, respectively. Then the distribution of a_i and $\overline{a}_i$ is multinomial distribution, and the counter value T_j of **Step 2** is

$$T_j = \sum_{i \in B_j} a_i + \sum_{i \notin B_j} \overline{a}_i. \tag{35}$$

In particular, if $j = j'$ then

$$T_{j'} = \sum_{i \in B} a_i. \tag{36}$$

For the success of Algorithm 2, we must have $|T_{j'} - N/2| > |T_j - N/2|$ for all j except j', and under our assumption this is equivalent to

$$T_{j'} > N - T_j \ \ \textit{and}\ \ T_{j'} > T_j. \tag{37}$$

Since

$$N = \sum_{i \in B} (a_i + \overline{a}_i), \tag{38}$$

we see that equation (37) is also equivalent to

$$\sum_{i \in B_j} (a_i - \overline{a}_i) > 0, \ and \ \sum_{i \notin B_j} (a_i - \overline{a}_i) > 0. \tag{39}$$

Therefore, the success rate of Algorithm 2 is

$$\sum_R \frac{N!}{a_0!a_1!, ..., a_{2^t-1}!\overline{a}_0!\overline{a}_1!, ..., \overline{a}_{2^t-1}!} {p_0}^{a_0} {p_1}^{a_1}, ..., {p_{2^t-1}}^{a_{2^t-1}} {\overline{p}_0}^{\overline{a}_0} {\overline{p}_1}^{\overline{a}_1}, ..., {\overline{p}_{2^t-1}}^{\overline{a}_{2^t-1}}, \tag{40}$$

where the region R is given by the following form:

$$\begin{aligned} R \ = \ \{ \ & (a_0, a_1, ..., a_{2^t-1}, \overline{a}_0, \overline{a}_1, ..., \overline{a}_{2^t-1}) \mid 0 \le \forall j (\ne j') < 2^k, \\ & \sum_{i \in B_j} (a_i - \overline{a}_i) > 0, \ \sum_{i \notin B_j} (a_i - \overline{a}_i) > 0, \ \sum_{i \in B} (a_i + \overline{a}_i) = N \ \}. \end{aligned} \tag{41}$$

We now change variables from a_i and $\overline{a}_i$ to $x_i = \frac{a_i - Np_i}{\sqrt{N}}$ and $\overline{x}_i = \frac{\overline{a}_i - N\overline{p}_i}{\sqrt{N}}$, respectively, and then according to Stirling's formula, we can finally reach equation (42). We omit the detailed derivation of this transformation, since our approach is based on the general method used when approximating multinomial distribution by normal distribution:

$$\begin{aligned} & \overbrace{\int\int ... \int_{R'}}^{2^{t+1}-1} \frac{1}{(2\pi)^{(2^{t+1}-1)/2} \prod_{i=0}^{2^t-1} (\sqrt{p_i \overline{p}_i})} \ exp \ (-\frac{1}{2} \sum_{i=0}^{2^t-1} (\frac{{x_i}^2}{p_i} + \frac{{\overline{x}_i}^2}{\overline{p}_i}) \ ) \\ & \qquad dx_0 dx_1 ... dx_{2^t-1} d\overline{x}_0, d\overline{x}_1 ... d\overline{x}_{2^t-2}, \end{aligned} \tag{42}$$

where the region R' is represented as follows:

$$\begin{aligned} R' \ = \ \{ \ & (x_0, x_1, ..., x_{2^t-1}, \overline{x}_0, \overline{x}_1, ..., \overline{x}_{2^t-1} \ ) \mid 0 \le \forall j (\ne j') < 2^k, \\ & \sum_{i \in B_j} (\sqrt{N}(p_i - \overline{p}_i) + (x_i - \overline{x}_i)) > 0, \\ & \sum_{i \notin B_j} (\sqrt{N}(p_i - \overline{p}_i) + (x_i - \overline{x}_i)) > 0, \ \sum_{i \in B} (x_i + \overline{x}_i) = 0 \ \}. \end{aligned} \tag{43}$$

According to our hypothesis, p_i and $\overline{p}_i$ are sufficiently close to $2^{-(t+1)}$. Moreover, we have $p_i - \overline{p}_i = (p - 1/2)/2^{t-1}$. This completes our assertion. □

This lemma guarantees that the probabilistic behavior of equation (33) is the same as that of equation (26); in other words, the probability that equation (33) of 16-round DES is solvable with, for example, 2^{45} random plaintexts is the same as the probability that equation (26) of 8-round DES is solvable with $2^{45}|1.19 \times 2^{-21}|^2/|1.95 \times 2^{-9}|^2 = 1.49 \times 2^{19}$ random plaintexts. Our computer experiments of 8-round DES tell us the expected success rates of 16-round DES as follows:

N	2^{43}	2^{44}	2^{45}
Success Rate	32.5%	77.7%	99.4%

Table 8. Expected results of the experiments to solve equation (33).

According to round symmetry of DES, we have another best expression of 16-round DES which holds with the same probability as equation (33):

$$\begin{aligned} & C_H[7,18,24] \oplus F_{16}(C_L, K_{16})[7,18,24] \oplus P_H[15] \oplus P_L[7,18,24,29] \oplus F_1(P_L, K_1)[15] \\ & = K_{14}[22] \oplus K_{13}[44] \oplus K_{12}[22] \oplus K_{10}[22] \ \oplus K_9[44] \oplus K_8[22] \oplus K_6[22] \oplus K_5[44] \oplus \\ & \quad K_4[22] \oplus K_2[22]. \end{aligned} \tag{44}$$

This equation gives us $K_1[42] \sim K_1[47]$, $K_{16}[18] \sim K_{16}[23]$ and one subkey bit of the right side of equation (44). In this stage, we have 26 subkey bits, which correspond to the following 26 secret key bits.

$$0,1,3,4,8,9,14,15,18,19,24,25,31,32,38,39,41,42,44,45,50,51,54,55,$$
$$5 \oplus 13 \oplus 17 \oplus 20 \oplus 46, \quad 2 \oplus 7 \oplus 11 \oplus 22 \oplus 26 \oplus 37 \oplus 52.$$

The remaining $56 - 26 = 30$ secret key bits are now easily obtained by an exhaustive search. As a result, the total success rate of our attack is now expected as the following table, where each entry shows the squared value of that of Table 8, since we have to solve two independent equations.

N	2^{43}	2^{44}	2^{45}
Success Rate	10.6%	60.4%	98.8%

Table 9. Expected results of the experiments to break 16-round DES.

7 Concluding Remarks

We have introduced a new methodology for cryptanalysis based on linear approximation of block ciphers. We have completely determined the best linear approximate expression and its probability for DES, and applied this method to a known-plaintext attack. As a result, 16-round DES is breakable faster than an exhaustive key search using 2^{45} random known-plaintexts and the corresponding ciphertexts. Moreover, our analysis is applicable to a ciphertexts-only attack.

As for the best expression and the best probability of DES, it is impossible to have better results, since we have made a complete search without any assumption. As for the known-plaintext attack, however, we do not know whether Algorithm 2 is the best method to solve equation (2), because Algorithm 2 derives subkeys without any information on the structure of S-boxes. It may hence be possible that faster attacks are found.

Acknowledgments

The author would like to thank Dr. E.Biham, Prof. M.Hellman, Dr. K. Ohta, Dr. R.Rueppel and Prof. A.Shamir for helpful comments on earlier versions of this paper.

References

[1] E.Biham and A.Shamir, Differential Cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, vol.4, no.1, 1991, pp.3–72.

[2] E.Biham and A.Shamir, Differential Cryptanalysis of the full 16-round DES, *Abstracts of Crypto'92*, 1992, pp.12-1–12-5.

[3] Y.Desmedt, J.J.Quisquater and M.Davio, Dependence of output on input in DES: Small avalanche characteristics, *Proceedings of Crypto'84 — Advances in Cryptology*, Lecture notes in Computer Science, vol.196, Springer-Verlag, 1984, pp.359–376.

[4] M.Hellman, R.Merkle, R.Schroeppel, L.Washington, W.Diffie, S.Pohlig, and P.Schweitzer, Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard, Information Systems Laboratory, SEL 76-042, Stanford University, 1976.

[5] M.Matsui, Linear Cryptanalysis of DES cipher (II), in preparation.

[6] National Bureau of Standards, *Data Encryption Standard*, Federal Information Processing Standards, no.16, U.S.Department of Commerce, 1977.

[7] R.A.Rueppel, *Analysis and design of stream ciphers*, Springer Verlag, 1986.

[8] A.Shamir, On the security of DES, *Proceedings of Crypto'85 — Advances in Cryptology*, Lecture notes in Computer Science, vol.218, Springer-Verlag, 1985, pp.280–281.

$i \setminus j$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	39	7	47	15	55	23	63	31	38	6	46	14	54	22	62	30
16	37	5	45	13	53	21	61	29	36	4	44	12	52	20	60	28
32	35	3	43	11	51	19	59	27	34	2	42	10	50	18	58	26
48	33	1	41	9	49	17	57	25	32	0	40	8	48	16	56	24

Annex A-1: The initial permutation IP.

$i \setminus j$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
16	61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7
32	56	48	40	32	24	16	8	0	58	50	42	34	26	18	10	2
48	60	52	44	36	28	20	12	4	62	54	46	38	30	22	14	6

Annex A-2: The final permutation IP^{-1}.

$i \setminus j$	0	1	2	3	4	5	6	7
0	1,47	2	3	4, 6	5, 7	8	9	10,12
8	11,13	14	15	16,18	17,19	20	21	22,24
16	23,25	26	27	28,30	29,31	32	33	34,36
24	35,37	38	39	40,42	41,43	44	45	46, 0

Annex A-3: The extension E.

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

Annex A-4: The permutation P.

$i \setminus j$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	-	27	19	11	31	39	47	55	-	26	18	10	30	38	46	54
16	-	25	17	9	29	37	45	53	-	24	16	8	28	36	44	52
32	-	23	15	7	3	35	43	51	-	22	14	6	2	34	42	50
48	-	21	13	5	1	33	41	49	-	20	12	4	0	32	40	48

Annex A-5: The permutation PC-1.

In annexes A-1 $\sim$ A-5, each entry shows the output bit position corresponding to the $(i+j)$-th input bit position.

	$i \setminus j$	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
S_1	00	e	0	4	f	d	7	1	4	2	e	f	2	b	d	8	1
	10	3	a	a	6	6	c	c	b	5	9	9	5	0	3	7	8
	20	4	f	1	c	e	8	8	2	d	4	6	9	2	1	b	7
	30	f	5	c	b	9	3	7	e	3	a	a	0	5	6	0	d

	$i \setminus j$	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
S_2	00	f	3	1	d	8	4	e	7	6	f	b	2	3	8	4	e
	10	9	c	7	0	2	1	d	a	c	6	0	9	5	b	a	5
	20	0	d	e	8	7	a	b	1	a	3	4	f	d	4	1	2
	30	5	b	8	6	c	7	6	c	9	0	3	5	2	e	f	9

	$i \setminus j$	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
S_3	00	a	d	0	7	9	0	e	9	6	3	3	4	f	6	5	a
	10	1	2	d	8	c	5	7	e	b	c	4	b	2	f	8	1
	20	d	1	6	a	4	d	9	0	8	6	f	9	3	8	0	7
	30	b	4	1	f	2	e	c	3	5	b	a	5	e	2	7	c

	$i \setminus j$	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
S_4	00	7	d	d	8	e	b	3	5	0	6	6	f	9	0	a	3
	10	1	4	2	7	8	2	5	c	b	1	c	a	4	e	f	9
	20	a	3	6	f	9	0	0	6	c	a	b	1	7	d	d	8
	30	f	9	1	4	3	5	e	b	5	c	2	7	8	2	4	e

	$i \setminus j$	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
S_5	00	2	e	c	b	4	2	1	c	7	4	a	7	b	d	6	1
	10	8	5	5	0	3	f	f	a	d	3	0	9	e	8	9	6
	20	4	b	2	8	1	c	b	7	a	1	d	e	7	2	8	d
	30	f	6	9	f	c	0	5	9	6	a	3	4	0	5	e	3

	$i \setminus j$	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
S_6	00	c	a	1	f	a	4	f	2	9	7	2	c	6	9	8	5
	10	0	6	d	1	3	d	4	e	e	0	7	b	5	3	b	8
	20	9	4	e	3	f	2	5	c	2	9	8	5	c	f	3	a
	30	7	b	0	e	4	1	a	7	1	6	d	0	b	8	6	d

	$i \setminus j$	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
S_7	00	4	d	b	0	2	b	e	7	f	4	0	9	8	1	d	a
	10	3	e	c	3	9	5	7	c	5	2	a	f	6	8	1	6
	20	1	6	4	b	b	d	d	8	c	1	3	4	7	a	e	7
	30	a	9	f	5	6	0	8	f	0	e	5	2	9	3	2	c

	$i \setminus j$	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
S_8	00	d	1	2	f	8	d	4	8	6	a	f	3	b	7	1	4
	10	a	c	9	5	3	6	e	b	5	0	0	e	c	9	7	2
	20	7	2	b	1	4	e	1	7	9	4	c	a	e	8	2	d
	30	0	f	6	c	a	9	d	0	f	3	3	5	5	6	8	b

Annex A-6: The S-boxes S_a. (Each entry shows $S_a(i+j)$ in hexadecimal form.)

i	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}	K_{16}
0	23	22	20	18	16	14	12	10	9	7	5	3	1	27	25	24
1	26	25	23	21	19	17	15	13	12	10	8	6	4	2	0	27
2	19	18	16	14	12	10	8	6	5	3	1	27	25	23	21	20
3	5	4	2	0	26	24	22	20	19	17	15	13	11	9	7	6
4	13	12	10	8	6	4	2	0	27	25	23	21	19	17	15	14
5	9	8	6	4	2	0	26	24	23	21	19	17	15	13	11	10
6	2	1	27	25	23	21	19	17	16	14	12	10	8	6	4	3
7	21	20	18	16	14	12	10	8	7	5	3	1	27	25	23	22
8	27	26	24	22	20	18	16	14	13	11	9	7	5	3	1	0
9	16	15	13	11	9	7	5	3	2	0	26	24	22	20	18	17
10	6	5	3	1	27	25	23	21	20	18	16	14	12	10	8	7
11	11	10	8	6	4	2	0	26	25	23	21	19	17	15	13	12
12	7	6	4	2	0	26	24	22	21	19	17	15	13	11	9	8
13	22	21	19	17	15	13	11	9	8	6	4	2	0	26	24	23
14	10	9	7	5	3	1	27	25	24	22	20	18	16	14	12	11
15	4	3	1	27	25	23	21	19	18	16	14	12	10	8	6	5
16	15	14	12	10	8	6	4	2	1	27	25	23	21	19	17	16
17	25	24	22	20	18	16	14	12	11	9	7	5	3	1	27	26
18	0	27	25	23	21	19	17	15	14	12	10	8	6	4	2	1
19	8	7	5	3	1	27	25	23	22	20	18	16	14	12	10	9
20	18	17	15	13	11	9	7	5	4	2	0	26	24	22	20	19
21	24	23	21	19	17	15	13	11	10	8	6	4	2	0	26	25
22	3	2	0	26	24	22	20	18	17	15	13	11	9	7	5	4
23	14	13	11	9	7	5	3	1	0	26	24	22	20	18	16	15
24	53	52	50	48	46	44	42	40	39	37	35	33	31	29	55	54
25	42	41	39	37	35	33	31	29	28	54	52	50	48	46	44	43
26	35	34	32	30	28	54	52	50	49	47	45	43	41	39	37	36
27	28	55	53	51	49	47	45	43	42	40	38	36	34	32	30	29
28	48	47	45	43	41	39	37	35	34	32	30	28	54	52	50	49
29	39	38	36	34	32	30	28	54	53	51	49	47	45	43	41	40
30	47	46	44	42	40	38	36	34	33	31	29	55	53	51	49	48
31	29	28	54	52	50	48	46	44	43	41	39	37	35	33	31	30
32	51	50	48	46	44	42	40	38	37	35	33	31	29	55	53	52
33	43	42	40	38	36	34	32	30	29	55	53	51	49	47	45	44
34	36	35	33	31	29	55	53	51	50	48	46	44	42	40	38	37
35	32	31	29	55	53	51	49	47	46	44	42	40	38	36	34	33
36	45	44	42	40	38	36	34	32	31	29	55	53	51	49	47	46
37	34	33	31	29	55	53	51	49	48	46	44	42	40	38	36	35
38	49	48	46	44	42	40	38	36	35	33	31	29	55	53	51	50
39	40	39	37	35	33	31	29	55	54	52	50	48	46	44	42	41
40	55	54	52	50	48	46	44	42	41	39	37	35	33	31	29	28
41	52	51	49	47	45	43	41	39	38	36	34	32	30	28	54	53
42	50	49	47	45	43	41	39	37	36	34	32	30	28	54	52	51
43	54	53	51	49	47	45	43	41	40	38	36	34	32	30	28	55
44	31	30	28	54	52	50	48	46	45	43	41	39	37	35	33	32
45	44	43	41	39	37	35	33	31	30	28	54	52	50	48	46	45
46	38	37	35	33	31	29	55	53	52	50	48	46	44	42	40	39
47	41	40	38	36	34	32	30	28	55	53	51	49	47	45	43	42

Annex A-7: The key-scheduling part. (Each entry shows the secret key bit position corresponding to the subkey bit position $K_j[i]$.)

$\alpha \setminus \beta$	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	-2	-2	-4	-2	0	-4	6	2	0	0	6	4	-2	-6	4
03	-2	-2	-4	-2	0	-4	6	2	8	0	-2	4	6	-6	-4
04	2	-2	-4	-2	0	-4	-6	-2	4	8	2	0	-2	-6	12
05	-2	-2	0	-2	-4	-4	-2	2	-4	-4	2	4	-10	-2	-4
06	0	0	4	0	4	0	0	0	-4	4	4	0	0	-4	-8
07	-4	0	8	0	0	0	4	4	-4	-8	-4	4	0	0	0
08	4	-2	6	-6	-6	0	-4	-4	-4	2	-2	2	-2	0	0
09	0	6	-6	-2	-6	4	-4	0	-4	-2	6	2	-6	0	-4
10	-2	0	2	0	6	8	2	-2	0	-2	4	-2	0	-2	4
11	2	-8	-2	-4	-10	4	2	-6	8	2	4	-2	-4	-2	0
12	-2	0	6	0	2	0	2	2	0	6	-4	2	-4	6	0
13	6	0	6	4	-2	-4	-2	2	0	6	4	-2	8	-6	-4
14	0	-2	-2	2	2	0	0	4	4	6	-2	2	2	-4	4
15	0	-2	6	-2	-2	4	-4	-4	-4	-2	-2	-2	-2	0	0
16	2	2	0	-2	0	4	-6	0	6	2	-4	6	-4	-4	-18
17	2	-2	-4	2	-4	-4	10	-4	2	2	-4	-2	-4	0	-6
18	4	0	0	-4	4	0	4	-6	2	2	6	2	6	6	-10
19	4	-4	-4	0	0	-8	-12	-2	-2	-6	6	2	6	2	2
20	4	0	4	-8	-4	4	0	2	6	-2	2	6	2	-2	2
21	0	4	-4	-4	4	4	-4	10	2	2	2	-6	2	6	-2
22	6	2	0	2	-4	0	2	4	2	2	0	-2	0	0	2
23	2	6	-8	6	4	0	-2	-12	-2	-2	0	-6	0	0	-2
24	2	8	2	0	6	4	2	4	-2	4	6	0	-2	-4	2
25	-2	4	-6	0	-6	0	2	4	-6	8	6	0	2	0	-6
26	0	-6	2	-2	-2	4	4	-2	-2	0	0	-4	4	2	2
27	4	6	2	-10	2	-8	4	-2	-6	4	0	4	0	-2	2
28	-4	2	2	2	-6	0	-4	-2	-2	4	0	0	4	2	2
29	4	-2	-2	2	-6	-4	0	2	2	-4	0	-12	0	-6	-6
30	2	0	-2	4	-2	0	-2	0	6	-4	-2	0	-2	0	2
31	2	-4	2	-4	-2	4	2	4	-6	4	-2	-4	2	0	2
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	2	-2	0	2	0	0	6	-2	0	-4	6	4	10	10	0
35	2	-2	0	2	0	0	6	6	0	4	-10	-4	-6	2	0
36	2	-6	-8	2	4	4	2	2	0	0	2	0	6	-10	0
37	-2	2	4	2	0	-4	-2	-2	0	4	2	-4	6	-6	0
38	4	4	-4	8	-8	4	0	0	-8	0	-4	0	4	0	0
39	0	-4	-8	-8	4	-4	-4	4	-8	-4	-4	4	4	-4	0
40	4	-2	-2	-2	-2	-4	0	4	4	2	6	-2	-6	12	4
41	0	-2	-6	2	-2	-8	8	0	-4	-2	-2	6	-2	-4	0
42	2	0	-2	0	2	0	-2	2	-8	-6	-4	2	0	2	-4
43	-10	0	2	-4	2	4	6	-2	0	-10	4	2	-4	-6	0
44	6	-4	2	8	2	4	6	-2	-4	-2	12	-2	-8	-2	0
45	-2	-4	2	-4	-2	0	2	-2	-4	-2	4	-6	4	2	-4
46	-4	2	6	6	-6	-8	4	-4	0	2	6	6	2	4	0
47	-4	2	-2	2	-10	12	0	-4	0	2	-2	10	6	0	4
48	-2	-2	0	-2	4	0	2	0	2	6	4	6	0	0	-2
49	-2	2	4	2	0	0	-6	-4	-2	-2	-4	-2	0	-4	2
50	-4	-4	-4	0	0	0	4	-2	-2	-6	-2	-6	6	2	2
51	-4	0	0	4	-4	0	-4	-6	2	2	-2	2	-2	-2	-2
52	8	-8	8	4	4	0	0	-2	-2	2	-6	6	6	-2	-2
53	4	-4	0	-8	-4	0	-4	-2	2	-2	2	2	-2	-2	2
54	6	2	-8	2	-4	8	2	4	-6	2	0	6	0	0	2
55	2	-10	0	6	4	8	-2	4	6	-2	0	2	0	0	-2
56	-10	4	2	-4	-2	4	-2	4	2	0	6	-4	6	-4	-2
57	2	0	-6	-4	2	0	-2	-4	6	-4	-2	4	2	8	-2
58	0	6	-2	6	6	0	0	2	2	0	0	8	0	2	2
59	4	2	-2	-2	10	4	0	-14	-2	4	0	0	-4	-2	2
60	0	10	-2	-6	-2	0	8	-6	6	0	-8	-4	4	-2	2
61	8	-2	2	-6	-2	4	4	-2	-6	0	0	0	0	-2	2
62	2	0	-2	-8	2	4	2	0	-2	4	-2	-4	2	4	-2
63	-14	-12	-6	0	2	0	-2	-4	-6	12	-2	0	-2	4	-2

Annex B-1: The table of $NS_1(\alpha, \beta) - 32$.

$\alpha \setminus \beta$	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	0	0	4	0	0	-4	0	0	0	-4	0	0	0	0	4
03	0	4	-8	0	8	0	-4	0	0	-8	-4	0	8	-4	8
04	-2	2	4	2	0	4	6	0	6	-2	0	2	0	0	10
05	2	2	0	2	-4	4	-6	0	-6	6	4	-6	4	0	-2
06	-2	-2	-4	-2	-4	0	-2	-4	2	2	0	2	0	4	10
07	2	2	-4	-2	0	4	-2	-4	6	6	0	-6	-4	0	2
08	0	2	2	-2	2	4	0	-2	-6	-4	0	0	0	10	-6
09	0	-2	-2	-2	2	8	4	-2	2	0	-4	0	8	-10	-2
10	-4	2	2	2	2	-4	-8	2	2	4	0	0	4	-6	2
11	4	2	10	2	2	4	0	2	2	4	0	0	-4	2	2
12	-2	4	-2	0	2	0	6	-2	0	2	0	2	0	-6	-4
13	-6	0	-2	0	6	4	-10	6	-4	6	0	2	-4	-2	4
14	-6	0	2	0	-2	-8	6	-2	4	2	0	2	4	-2	0
15	-2	0	-2	0	2	0	10	6	8	2	4	2	0	-2	4
16	0	-4	4	0	0	0	0	0	0	4	4	4	-12	-4	-12
17	0	0	0	0	-8	4	4	0	0	8	0	-4	4	8	0
18	0	0	4	0	8	0	4	0	0	-4	8	-4	-12	0	12
19	0	-8	4	0	8	8	4	0	0	-4	0	4	-4	8	-4
20	-2	-6	-4	-2	4	-4	-2	-4	2	2	-4	6	-4	0	2
21	10	-2	-4	-2	0	0	-2	4	6	6	-4	-2	0	4	2
22	-2	-6	0	2	0	4	2	8	-2	2	0	6	4	0	-2
23	10	2	4	2	4	-4	-2	0	2	2	-4	-2	0	0	2
24	-4	2	-2	2	2	4	4	-2	-2	4	4	0	4	-2	2
25	4	-6	6	2	2	4	-4	-2	-2	4	-4	8	4	-2	2
26	8	-2	2	-2	2	0	0	2	6	0	0	0	0	2	-2
27	-8	10	6	-2	2	4	-4	2	-2	-4	-4	-8	0	-2	-6
28	2	8	-2	0	-2	0	2	2	0	-6	4	10	-4	2	0
29	-2	0	2	0	-6	0	-2	2	4	2	0	10	0	2	4
30	-2	0	6	0	2	4	-2	2	4	-2	0	2	0	2	0
31	2	-4	6	0	-2	-8	-2	-14	0	2	0	2	4	-2	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	4	0	-8	4	0	0	0	-4	-16	0	-8	-8	4
35	0	-4	0	0	0	0	4	0	0	0	4	0	0	-4	0
36	-2	-2	0	-2	-4	4	-10	0	6	-6	-4	6	4	8	2
37	-6	-2	4	-2	0	4	2	0	2	2	-8	-2	0	8	-2
38	6	-6	0	-14	0	0	-2	-4	-6	-2	4	-2	-4	-4	2
39	2	6	0	2	-4	-4	-2	-4	6	-6	4	6	0	0	-6
40	-4	2	-2	2	2	0	-8	2	2	0	8	8	-4	-6	-2
41	-4	-2	-6	2	2	4	-4	-6	2	-4	-4	0	-4	-2	-6
42	8	2	-2	6	-6	0	0	-2	2	0	0	0	0	-6	-2
43	0	-6	-2	6	10	0	0	-10	10	0	0	-8	0	2	-2
44	-6	0	6	0	-2	-4	-2	2	-8	2	4	-2	0	2	8
45	-2	-4	-2	0	-6	0	-10	2	4	-2	4	-10	-4	-2	0
46	-2	-4	2	8	2	4	-2	-6	-4	-6	4	-2	4	-2	4
47	-6	4	-2	-8	-2	4	2	-6	0	10	0	6	0	-2	0
48	0	-4	4	-4	-4	4	4	0	0	-4	-4	0	0	-8	0
49	0	0	0	4	-4	0	0	0	0	0	-8	0	-8	-4	4
50	0	0	4	4	4	4	0	0	0	4	0	0	0	-4	0
51	0	0	-4	-4	-4	-4	0	0	0	-4	0	0	0	4	0
52	-10	-2	-8	6	4	-8	2	4	2	6	-8	-2	-4	4	-2
53	-6	2	0	-2	0	4	2	-4	-2	-6	0	-2	0	0	-2
54	-2	-2	4	-6	0	8	-2	0	6	6	4	-2	4	-4	2
55	2	-2	-8	-14	4	0	2	8	2	-2	0	-2	0	-4	-2
56	0	2	2	-6	-2	-4	0	2	-2	0	-4	-4	-4	2	2
57	8	10	-6	2	6	4	0	-6	-10	8	-4	4	-4	2	2
58	-4	-2	6	-2	-2	-8	4	-2	-2	4	0	-4	0	-2	-2
59	-4	2	2	-10	6	-4	0	-10	-2	0	-4	4	0	2	2
60	-2	-4	-2	4	-2	0	-2	-2	0	2	0	2	-8	-2	0
61	2	4	10	-4	10	-8	-6	6	4	2	-4	2	4	-2	-4
62	2	-12	-2	4	2	-4	2	6	-12	-2	-4	2	4	-2	0
63	-2	-8	-2	-4	-2	0	-6	-2	0	2	4	2	0	2	0

Annex B-2: The table of $NS_2(\alpha, \beta) - 32$.

$\alpha \setminus \beta$	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	2	-2	-4	0	-2	-6	4	0	6	-2	-8	4	-2	-2	-4
03	-2	-2	0	4	-2	-2	-4	-4	-2	2	0	-4	2	-2	0
04	-4	0	0	2	-2	-6	2	0	4	4	-4	-6	-10	6	-2
05	0	0	-4	2	2	2	6	0	0	4	0	2	-6	6	2
06	-2	2	0	2	-4	0	2	0	-6	-2	0	-2	4	8	-2
07	-2	2	0	-2	8	4	6	-4	-2	2	-4	-10	4	0	-2
08	0	6	-6	0	0	2	-2	-2	2	0	8	6	2	4	-4
09	0	2	-2	0	-8	-2	-6	-2	2	-4	-4	-2	2	8	0
10	-2	8	-2	0	2	-8	-6	2	0	6	4	-2	0	2	-4
11	2	-4	6	4	2	0	-2	-2	0	-2	0	-2	-4	-2	4
12	0	-2	-2	2	10	4	-4	2	-2	0	-4	4	-8	6	-6
13	-4	2	-2	2	-2	0	12	2	2	4	4	4	4	2	2
14	-2	-4	-2	2	-4	-2	-4	-2	4	2	4	4	-2	-8	-2
15	-2	-8	2	-2	0	-2	-4	-6	-8	2	4	4	-2	4	2
16	0	2	-2	2	2	8	4	2	6	-4	12	-4	-8	2	10
17	0	-2	2	-2	-2	0	4	-2	2	4	-4	4	0	-10	6
18	-2	4	2	-2	0	2	4	-2	-4	-6	0	0	-14	4	-2
19	2	0	2	-2	4	-2	-12	-2	0	-2	8	-8	-2	0	-2
20	4	-6	-2	-4	0	2	-2	2	-6	-8	0	6	-2	0	0
21	8	-2	6	0	8	2	2	-2	2	-8	-4	-2	2	4	0
22	2	0	-10	0	6	0	2	-2	0	2	0	2	0	-2	0
23	10	4	-6	0	-2	-4	-2	-2	0	-2	4	2	0	2	-4
24	0	4	-4	2	2	-2	-2	-4	4	4	4	-2	6	6	-2
25	8	-4	-4	-2	-2	2	2	0	0	0	8	-10	-2	-10	-2
26	-6	2	0	-2	4	-4	-2	-4	2	2	4	6	0	0	-2
27	-2	2	-4	-2	0	-4	2	4	-2	2	0	-2	4	0	2
28	0	-4	0	-4	4	-8	4	0	-8	4	0	-4	4	8	4
29	4	4	4	0	4	-4	-4	4	8	0	0	4	0	0	8
30	-6	6	0	0	-2	2	0	-8	-2	-2	-4	4	-2	-2	0
31	-6	-10	0	0	6	-6	0	0	-2	-2	4	4	-2	-2	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	-2	-2	0	0	2	2	-8	0	2	-2	-4	4	2	6	16
35	2	-2	-4	4	-6	6	-8	-4	2	2	-4	-4	-2	6	-4
36	4	0	8	2	-2	-6	2	4	0	-8	8	6	2	2	-6
37	0	0	-4	2	-6	2	-2	4	4	8	4	-2	-2	2	6
38	2	-6	-12	2	0	0	-2	-4	-6	2	0	2	-4	-4	-2
39	2	-6	4	-2	-4	4	2	8	-2	6	-4	-6	-4	4	-2
40	0	2	-2	0	8	6	2	-2	-6	-4	4	-2	10	0	0
41	0	-2	2	0	0	2	-2	-2	-6	8	8	6	-6	4	4
42	2	4	-2	8	-2	-4	2	2	-4	2	-4	-2	-4	-2	4
43	-2	8	-2	-4	-10	4	-2	-2	-12	-6	0	-2	0	-6	4
44	0	2	-6	2	10	0	0	-2	2	0	-4	0	-4	-2	2
45	4	6	2	2	6	-4	-8	-2	-2	4	-4	0	0	-6	2
46	2	-8	-2	-6	0	2	-4	2	4	2	0	0	-2	0	-6
47	2	4	2	6	4	2	-4	14	-8	2	0	0	-2	-4	-2
48	0	-6	-2	-2	-2	-4	0	2	-2	4	4	0	4	-2	6
49	0	-2	-6	2	2	4	0	-2	-6	4	-4	0	4	2	2
50	2	-4	-2	2	0	6	4	-2	8	2	4	-4	2	0	-2
51	-2	0	-2	-6	4	2	-4	-2	4	-2	-4	-4	-2	-4	6
52	-4	2	6	0	4	-2	2	6	-2	4	4	-2	-2	0	0
53	8	-2	-2	12	-4	-2	-2	2	-2	-4	0	-2	2	4	8
54	-2	0	2	-4	-2	-12	2	-6	0	-2	0	-6	-4	-2	4
55	6	-4	-2	-12	-2	0	-2	10	0	2	-4	2	4	2	0
56	0	0	8	6	-2	6	-2	-4	4	0	0	2	2	-2	-2
57	8	0	0	10	2	-6	2	0	0	4	-4	2	2	-2	-2
58	6	-2	0	2	4	-4	2	-4	-2	-2	4	-6	0	0	2
59	-14	-10	-4	10	0	-4	-2	4	2	-10	0	-6	4	0	-2
60	0	0	4	-8	0	0	-4	-4	4	4	0	-4	4	4	0
61	-4	0	8	4	0	4	-4	0	-4	8	0	-4	0	-4	-4
62	6	2	0	-4	-2	-6	4	-4	-2	-2	0	-4	-6	2	0
63	6	-6	8	4	-2	2	4	-12	-2	6	0	4	2	2	0

Annex B-3: The table of $NS_3(\alpha, \beta) - 32$.

$\alpha \setminus \beta$	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	0	4	0	4	0	0	0	0	0	0	4	0	4	0	0
03	-4	0	8	0	0	8	-4	-4	-8	0	0	-8	0	-4	0
04	-2	-2	0	-2	0	0	-10	2	0	0	-6	0	-6	10	0
05	2	-2	-4	2	0	-4	6	2	4	0	-10	4	10	6	0
06	-2	2	0	-2	-4	-4	2	-2	-4	4	2	0	-2	2	8
07	-2	-2	4	-2	12	0	-2	2	0	12	2	4	2	2	0
08	-4	0	0	0	0	0	4	4	0	0	0	0	0	-4	0
09	0	-4	-8	4	0	8	0	0	-8	0	4	8	-4	0	0
10	-4	-4	0	4	0	0	-4	-4	0	0	4	0	-4	-4	0
11	4	-4	0	-4	0	0	-4	-4	0	0	-4	0	-4	4	0
12	-2	2	0	-2	4	4	-6	-2	4	-4	10	0	-10	-6	-8
13	-2	-2	-4	-2	4	0	-10	2	0	4	-6	-4	-6	10	0
14	-2	-2	0	-2	0	0	-2	2	0	0	2	0	2	2	0
15	2	-2	4	2	0	4	-2	2	-4	0	-2	-4	2	-2	0
16	-2	-2	0	2	4	4	10	-2	4	-4	6	0	-6	10	8
17	2	-2	-4	-2	-4	0	-6	-2	0	-4	10	-4	10	6	0
18	2	-2	0	-2	0	0	-6	-2	0	0	10	0	10	6	0
19	2	2	-4	-2	0	4	-10	2	-4	0	-6	4	6	-10	0
20	4	-4	0	-4	0	0	4	-4	0	0	-4	0	-4	-4	0
21	4	4	8	-4	0	0	4	4	0	0	4	-8	-4	4	0
22	8	-4	0	4	8	-8	0	8	-8	-8	4	0	-4	0	0
23	4	8	8	8	0	0	-4	-4	0	0	0	8	0	4	0
24	2	-2	0	-2	0	0	2	-2	0	0	2	0	2	-2	0
25	2	2	4	-2	0	-4	-2	2	4	0	2	-4	-2	-2	0
26	-2	-2	0	2	-4	-4	2	-2	-4	4	-2	0	2	2	-8
27	2	-2	-12	-2	4	0	2	-2	0	4	2	-12	2	-2	0
28	-4	0	0	0	8	-8	4	-4	-8	-8	0	0	0	4	0
29	0	-4	-8	-4	0	0	0	0	0	0	4	-8	4	0	0
30	-8	0	0	0	0	0	0	8	0	0	0	0	0	0	0
31	0	-8	8	8	0	0	0	0	0	0	0	-8	0	0	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	4	0	0	0	-8	8	4	4	8	8	0	0	0	4	-16
35	0	4	0	4	0	0	0	0	0	0	4	0	4	0	0
36	2	2	0	-2	4	4	6	2	4	-4	2	0	-2	6	-8
37	-2	2	4	2	-4	0	-2	2	0	-4	6	4	6	2	0
38	-10	2	0	2	0	0	-2	10	0	0	-2	0	-2	2	0
39	-2	-10	4	10	0	4	2	-2	-4	0	-2	-4	2	2	0
40	0	4	0	-4	8	-8	0	0	-8	-8	-4	0	4	0	-16
41	-4	0	0	0	0	0	4	4	0	0	0	0	0	-4	0
42	4	-4	0	-4	0	0	-4	-4	0	0	-4	0	-4	4	0
43	4	4	0	-4	0	16	4	4	-16	0	-4	0	4	4	0
44	-2	2	0	2	0	0	-2	2	0	0	6	0	6	2	0
45	-2	-2	-4	2	0	-4	-6	-2	4	0	-2	4	2	-6	0
46	2	10	0	-10	-4	-4	-2	2	-4	4	2	0	-2	-2	8
47	-10	2	-4	2	-12	0	-2	10	0	-12	-2	-4	-2	2	0
48	-2	-2	0	-2	0	0	6	2	0	0	2	0	2	-6	0
49	2	-2	-4	2	0	4	-2	2	-4	0	6	4	-6	-2	0
50	-2	2	0	-2	4	4	2	-2	4	-4	-6	0	6	2	8
51	-2	-2	4	-2	4	0	6	2	0	4	2	4	2	-6	0
52	0	8	0	-8	8	8	0	0	8	-8	0	0	0	0	0
53	-8	0	0	0	8	0	0	8	0	8	0	0	0	0	0
54	0	-4	0	-4	0	0	0	0	0	0	4	0	4	0	0
55	4	0	8	0	0	0	-4	4	0	0	0	-8	0	-4	0
56	-10	2	0	-2	-4	-4	2	-10	-4	4	2	0	-2	2	-8
57	-2	-10	12	-10	-4	0	-2	2	0	-4	2	12	2	2	0
58	-2	-10	0	-10	0	0	-2	2	0	0	2	0	2	2	0
59	10	-2	4	2	0	-4	-2	10	4	0	-2	-4	2	-2	0
60	4	8	0	8	0	0	-4	-4	0	0	0	0	0	4	0
61	-8	4	8	-4	0	0	0	-8	0	0	-4	-8	4	0	0
62	-4	-4	0	4	8	8	-4	-4	8	-8	-4	0	4	-4	0
63	4	-4	0	-4	-8	0	4	-4	0	-8	-4	0	-4	-4	0

Annex B-4: The table of $NS_4(\alpha, \beta) - 32$.

$\alpha \setminus \beta$	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	4	-2	2	-2	2	-4	0	4	0	2	-2	2	-2	0	-4
03	0	-2	6	-2	-2	4	-4	0	0	-2	6	-2	-2	4	-4
04	2	-2	0	0	2	-2	0	0	2	2	4	-4	-2	-2	0
05	2	2	-4	0	10	-6	-4	0	2	-10	0	4	-2	2	4
06	-2	-4	-6	-2	-4	2	0	0	-2	0	-2	-6	-8	2	0
07	2	0	2	-2	8	6	0	-4	6	0	-6	-2	0	-6	-4
08	0	2	6	0	0	-2	-6	-2	2	4	-12	2	6	-4	4
09	-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
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	-4	-2	2	-2	2	-4	8	-4	0	-6	6	2	-2	-16	-12
35	0	-2	-2	6	-2	-4	4	0	0	-2	-2	-2	6	4	-4
36	-2	6	4	0	6	-2	4	4	-6	-2	4	0	14	2	0
37	6	2	0	0	6	2	0	-4	-6	2	-8	0	-2	6	-4
38	2	4	-2	-2	0	2	-4	4	-2	-4	-2	6	0	-2	0
39	-10	0	-2	6	4	6	-4	0	6	-12	2	2	0	6	-4
40	4	-2	-2	0	4	-6	2	2	-6	4	0	6	-2	-4	0
41	0	2	6	0	0	6	2	2	-2	-8	0	-2	-6	0	0
42	0	-4	-8	6	6	6	-6	6	2	-2	-2	-8	4	-4	4
43	8	0	4	6	-2	-6	6	2	6	-2	6	-4	0	4	4
44	2	4	-6	0	-6	0	6	-2	-4	2	-4	-2	4	6	0
45	-2	-4	-2	0	-2	-8	2	-2	0	-6	-8	-2	0	-2	4
46	6	2	-4	6	4	4	-2	-10	-8	0	-2	4	-2	2	0
47	6	-6	-4	6	-4	4	-2	2	4	4	-6	0	2	-2	-4
48	2	-2	0	-4	-6	-2	-4	4	2	2	0	0	2	2	4
49	2	-2	0	0	-2	2	0	0	-2	-2	-4	0	2	2	4
50	6	0	-2	-2	8	2	4	0	10	0	2	-2	4	2	0
51	-6	0	10	2	0	-2	-4	0	6	0	-10	2	4	-2	0
52	0	-12	4	-4	0	4	-8	-4	0	-4	0	-4	-4	0	0
53	-8	0	0	8	-4	4	0	0	-4	-4	0	4	4	-4	4
54	4	-2	-6	-2	-2	8	0	4	-4	-2	-2	6	2	-4	0
55	-8	-6	-6	-6	6	0	4	12	0	2	-2	2	2	4	-4
56	2	4	-6	0	-2	4	-2	-6	4	-6	0	6	4	-2	0
57	-2	8	2	-4	6	-4	-6	-2	-4	2	4	-2	0	2	0
58	6	-10	0	2	4	0	-2	6	-4	0	2	4	-2	-2	-4
59	-2	-6	-4	-10	0	-8	-2	-10	4	4	-2	0	2	-2	4
60	-8	-6	-2	0	-4	2	2	-6	2	4	0	10	-2	4	4
61	4	2	2	4	4	-2	2	-2	10	0	0	2	2	4	0
62	-4	4	-4	2	2	-2	2	2	-2	-2	-2	4	-4	0	4
63	-4	-4	-4	14	6	-6	-2	2	-2	6	-2	0	0	-4	0

Annex B-5: The table of $NS_5(\alpha, \beta) - 32$.

$\alpha \setminus \beta$	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	0	0	0	2	-6	2	-6	2	6	-2	2	-4	0	0	4
03	0	0	0	-2	-2	-2	-2	-2	-6	2	-2	4	8	0	4
04	0	2	-2	2	-2	8	0	2	2	0	4	4	8	6	-2
05	0	6	-6	2	6	4	-4	-2	-2	-8	4	8	4	-2	-10
06	4	-2	-2	0	0	2	-2	0	0	-2	2	-8	4	2	2
07	-4	2	2	4	-4	2	-2	0	0	2	-2	4	0	-6	2
08	2	-2	0	-4	-2	-2	-8	2	0	8	6	6	-4	0	-2
09	-2	6	4	0	6	2	0	-2	0	4	6	-2	0	0	10
10	2	2	4	2	4	-8	2	0	2	-2	0	-6	-4	4	-2
11	-2	-6	8	2	0	8	-2	0	-2	-10	4	2	0	-4	2
12	-2	0	2	2	-4	2	8	-4	-2	0	-2	-2	-4	2	4
13	2	4	2	-2	-4	2	4	4	2	-4	-2	2	12	10	0
14	2	0	6	-4	2	-4	-2	-2	0	-2	-4	-6	8	2	4
15	-2	4	-2	-4	6	0	-2	2	0	-2	0	-2	0	2	0
16	2	0	-2	0	2	-4	-14	-4	-2	-4	-6	0	2	-12	10
17	2	0	-2	4	-2	8	6	-4	-2	-4	-6	4	-2	0	-2
18	2	0	-2	-2	0	2	-8	-6	8	-2	8	-4	2	4	-2
19	2	0	-2	-2	0	-6	0	-2	4	-6	-4	0	-2	8	10
20	-2	2	0	2	-4	-4	-2	-2	-4	-4	2	-4	-2	-6	-4
21	6	-2	-4	6	-8	-4	-2	2	8	4	-6	-4	6	-2	0
22	-6	6	0	4	2	-6	0	0	-2	-2	4	0	2	-2	0
23	-6	2	4	-4	2	-2	4	0	6	-6	0	0	2	-6	4
24	0	-2	2	0	0	-2	2	-2	2	4	-4	2	-2	0	0
25	-12	-2	-10	-8	-4	6	-2	-6	-6	8	-4	-2	6	4	0
26	8	2	-2	2	2	-4	0	0	-8	6	2	-2	-2	-4	0
27	-4	2	2	6	2	0	0	-8	4	-2	-2	2	-2	0	0
28	0	0	0	-2	-6	2	-2	0	-4	4	8	2	-6	2	2
29	4	4	0	-2	-10	-2	-2	0	-8	-8	0	2	-2	-2	-6
30	4	8	-4	-4	-4	0	0	-2	2	-2	-6	6	-2	2	2
31	0	-4	4	0	-4	0	4	2	2	-2	-2	-2	2	-2	2
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	4	0	-4	-2	2	-2	10	2	-6	-2	14	0	0	4	12
35	4	0	-4	2	-2	2	6	-2	-2	2	-6	0	0	-4	4
36	0	-2	2	-2	2	0	-8	-2	-2	0	-4	4	0	10	2
37	0	2	-2	-2	-6	-4	4	2	2	0	4	0	4	-6	2
38	8	2	6	0	4	6	6	-4	0	6	-2	4	4	-6	-2
39	0	6	10	-4	-8	-2	-2	-12	8	2	2	0	0	2	-2
40	2	2	-4	0	2	-2	0	-2	4	0	-2	6	-12	4	2
41	-2	2	8	4	-6	-6	0	2	-4	-4	-2	6	0	4	-2
42	6	-2	4	2	0	-4	2	-4	-6	-2	-4	-2	4	4	2
43	2	-2	0	10	4	-4	-2	4	-2	6	0	6	8	4	-2
44	-2	8	-6	2	4	2	0	4	-2	0	-10	-2	-4	2	4
45	2	4	2	-2	4	-6	4	-4	2	4	-2	2	-4	2	-8
46	6	-8	-6	0	-6	0	-2	6	4	-2	0	6	0	-2	4
47	2	4	10	-8	6	4	-2	10	4	6	-4	2	0	-2	0
48	2	0	-2	0	2	4	-6	0	2	0	-2	-4	-2	8	-2
49	2	0	-2	4	-2	0	-2	0	2	0	-2	0	-6	4	2
50	-2	0	2	2	-8	-2	0	-2	-8	2	0	-12	-2	4	-6
51	-2	0	2	-6	0	-2	0	2	4	-2	4	0	2	0	-2
52	-2	-2	4	-2	0	-4	-2	-2	-4	0	-2	8	2	2	4
53	-10	10	0	2	-4	-4	-2	10	0	0	-2	0	2	-2	0
54	-10	-6	0	-4	6	-2	0	0	-6	-6	-4	0	-2	2	0
55	6	6	4	-4	-2	10	-4	-8	-6	-2	0	0	-2	-2	4
56	0	-6	6	4	4	-2	-6	-2	-6	8	0	-2	2	0	0
57	4	2	2	-4	0	-2	-2	2	-6	-4	0	2	2	4	0
58	4	6	-2	-6	-2	-8	0	0	-4	2	2	6	2	0	0
59	8	-2	-6	-10	6	-4	0	0	0	-6	-2	-6	2	-4	-8
60	0	0	0	-2	2	2	6	-4	0	0	-4	-2	6	-2	-2
61	4	-4	8	-2	-2	6	-2	12	-4	-4	-4	-2	-6	2	-2
62	0	-8	0	8	4	-4	0	-6	2	-6	2	6	2	2	-2
63	-4	-12	0	-12	-4	-4	4	-2	2	2	-2	6	-2	-2	-2

Annex B-6: The table of $NS_6(\alpha, \beta) - 32$.

$\alpha \setminus \beta$	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	0	2	-6	4	-4	2	2	2	2	0	0	-2	-2	0	0
03	0	-2	6	0	0	2	-6	2	2	-4	-4	-6	2	0	8
04	0	2	2	0	-4	-6	-2	4	4	10	2	4	0	-6	6
05	0	2	10	0	4	-6	-2	0	-8	6	-2	0	-4	6	10
06	4	0	-4	-8	0	4	-4	-2	-6	-2	2	6	-2	2	-6
07	-4	4	0	4	4	-4	4	2	-2	6	2	6	-2	-2	-2
08	-4	0	4	-2	-2	-2	6	-4	4	0	0	-2	2	2	-2
09	4	-4	0	2	-6	-2	-10	0	0	0	0	-2	-6	-2	-6
10	0	-2	-10	2	-2	-4	0	2	6	0	4	0	0	2	2
11	0	-2	-2	10	-2	-4	0	6	-6	4	0	4	-4	-2	-2
12	0	-2	-2	2	-6	0	0	0	-4	-2	2	-2	-6	4	0
13	0	2	2	-2	-2	0	-8	0	4	2	-2	2	-2	-4	-8
14	0	0	0	2	2	6	-2	-2	-6	-6	6	-4	-8	-4	0
15	0	0	0	2	2	-2	6	6	-6	2	6	-4	0	4	0
16	-2	2	4	0	-2	-2	0	-2	4	4	6	-2	-4	8	-14
17	2	-2	4	-4	-2	-2	4	-2	0	0	-2	10	4	-8	-2
18	-2	0	2	-4	2	-4	-10	0	-2	0	-14	4	-6	4	-2
19	2	0	6	4	6	4	-6	0	-6	0	-2	-4	6	-4	-6
20	2	8	6	0	-10	4	-2	6	8	-2	-4	-2	-4	2	4
21	-2	-4	-2	4	-2	4	-6	2	0	-2	0	-2	0	-2	-4
22	-2	2	-4	-8	2	2	0	0	-2	-2	0	0	-6	-2	4
23	2	2	-8	-8	-10	2	-4	-12	6	2	0	4	2	2	4
24	2	-2	-4	2	0	-4	6	2	8	0	-6	0	2	2	-8
25	-2	6	-8	2	-4	-4	-6	6	0	12	2	-4	2	-2	0
26	-2	0	2	-2	0	-2	4	0	2	-4	2	2	0	-2	0
27	2	4	2	2	0	6	0	4	2	4	-2	2	4	2	0
28	2	0	-2	-2	8	2	0	2	0	6	0	-4	2	4	-2
29	-2	8	2	-2	-4	2	4	2	-4	-2	4	-12	-2	-4	-6
30	2	6	-4	-2	0	4	2	8	-2	-2	0	2	0	0	2
31	-2	2	4	2	0	4	-2	0	2	2	0	6	0	0	-2
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	2	2	-4	4	-6	2	2	2	0	-8	-2	-2	-16	-8
35	0	-2	-2	0	0	2	2	2	2	-4	4	2	-6	-8	8
36	0	-2	6	0	4	-2	2	-4	4	-2	6	4	0	-2	2
37	0	-2	-2	0	-4	-2	2	0	0	2	-6	-8	4	2	-2
38	-4	-4	0	-8	0	-8	0	6	2	2	6	-2	-2	-2	-2
39	-12	0	4	-4	-4	8	0	2	-2	2	-2	-2	-2	-6	2
40	0	-4	4	-2	-6	-6	-2	4	-8	-4	8	6	14	-2	-2
41	0	0	0	2	-2	2	-2	0	4	-4	0	-2	6	-6	2
42	-4	2	-2	2	2	0	0	-6	2	4	4	0	-4	-2	2
43	4	10	6	2	2	0	-8	6	6	-8	8	4	0	2	-2
44	4	6	2	2	-2	0	12	0	0	-2	-2	6	-10	4	-4
45	-4	2	6	-2	-6	-8	4	0	0	-6	-6	-6	2	4	4
46	4	0	4	-6	-2	6	2	-2	-2	2	2	4	4	4	-4
47	12	-8	4	2	-2	-2	2	6	6	2	2	-4	-4	-4	4
48	2	2	0	4	6	2	0	-2	8	4	2	2	4	-4	2
49	6	-2	0	0	6	2	4	-2	4	0	-6	-2	-4	-4	-2
50	2	0	6	0	-6	0	-2	0	2	0	6	0	-6	0	-2
51	6	0	-6	0	6	0	-6	0	-2	0	2	0	-2	0	2
52	-2	4	-2	-4	6	4	2	-2	4	2	4	-6	4	2	0
53	-6	-8	6	0	-2	4	-2	2	4	10	0	2	0	6	0
54	2	-2	4	-4	2	-6	-4	-8	2	2	8	-4	-6	-2	0
55	6	-2	0	4	-2	2	0	4	2	-2	0	0	2	2	0
56	2	-6	0	-2	4	4	-2	2	0	4	-2	-4	-2	2	0
57	6	-6	-4	-2	-8	-4	2	-2	-8	0	-2	0	-2	-2	0
58	6	4	-2	2	4	-10	-4	0	2	-8	-2	-2	4	6	0
59	2	0	-2	-18	4	-2	0	12	2	0	2	-2	0	2	0
60	-6	8	-2	2	4	-10	-4	-6	0	-2	0	0	-2	0	2
61	-2	-8	2	2	0	-2	0	-6	4	-2	4	-8	2	0	-2
62	-6	6	-4	2	-4	0	-2	0	-2	-2	0	-2	4	-4	-2
63	14	10	4	-2	-4	0	2	-8	-6	10	0	-6	4	-4	2

Annex B-7: The table of $NS_7(\alpha, \beta) - 32$.

$\alpha \setminus \beta$	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	2	0	-2	-2	0	2	0	-2	0	-2	4	-4	-2	0	6
03	-2	0	2	-2	4	-6	4	-2	-4	6	0	-4	2	0	2
04	-2	-2	0	0	2	-2	-4	2	0	4	-2	6	0	0	14
05	-2	-2	0	0	2	6	4	-2	12	-8	2	-6	4	4	2
06	0	2	2	2	6	0	-4	4	4	2	2	2	-2	4	-8
07	-4	2	-10	-6	2	8	0	0	-4	-2	2	-2	-2	0	0
08	0	2	-2	0	0	2	-2	-2	2	0	0	2	-2	4	-4
09	4	-2	-2	4	0	-6	2	2	2	0	12	-6	-6	0	-4
10	2	-2	0	2	4	-4	-2	0	-2	-2	4	6	-4	0	-2
11	2	2	12	6	8	4	-2	4	-6	-2	4	-2	-4	4	2
12	-2	0	-2	0	2	0	-6	0	2	-4	-10	0	6	4	-6
13	2	-4	-2	4	2	0	6	0	-2	0	6	-4	6	4	-2
14	0	0	4	-2	2	2	2	-2	-6	2	2	4	4	4	0
15	0	4	0	-6	-2	-6	2	-2	2	6	6	8	0	4	0
16	0	0	0	0	0	0	-8	0	0	0	0	0	-8	0	-16
17	0	0	0	0	-8	0	0	0	8	0	-8	0	8	0	0
18	2	0	-2	-2	0	2	8	-2	0	-2	4	-4	6	0	-10
19	-2	0	2	-2	-4	10	4	-2	4	-10	8	-4	-6	0	2
20	-2	-6	-4	4	-2	-2	-4	-2	4	-4	-2	-2	0	4	2
21	-2	2	4	-12	6	-2	4	-6	-8	-8	2	2	4	0	-2
22	0	6	-10	-2	-6	0	-4	8	0	-6	2	-6	-2	0	4
23	-4	-2	2	6	-2	0	0	4	0	-2	2	6	-2	4	4
24	-4	2	2	0	4	2	2	6	-2	0	-4	2	2	-4	-8
25	0	6	10	-4	4	-6	-2	2	-2	0	0	-6	-2	0	0
26	-2	6	-4	-6	0	-4	2	0	2	-2	0	6	0	0	2
27	-2	2	0	-10	4	4	-6	-4	-2	-2	-8	-2	0	-4	-2
28	-6	-4	-2	4	2	0	6	4	2	4	2	8	2	0	-6
29	-2	-8	-2	0	2	-8	2	-4	-2	0	2	4	2	0	-2
30	-4	-4	4	2	2	2	-2	2	-6	-6	-2	-4	0	0	0
31	-4	0	0	-10	-2	2	-2	-6	2	6	2	0	-4	0	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	-2	4	-2	2	0	-6	4	-2	-4	-6	-4	0	-2	16	2
35	2	-4	2	2	-4	-6	8	-2	0	-6	-8	0	-6	-8	-2
36	2	2	-8	0	6	2	4	-2	0	4	2	2	0	0	2
37	2	2	-8	0	6	-6	-4	2	4	0	-2	-2	-4	-4	-2
38	8	2	-6	-2	-6	-4	0	0	-8	6	-2	-6	-2	4	0
39	-4	-6	-2	-10	-2	-4	4	4	0	2	6	-2	-2	0	0
40	0	2	-2	0	0	-6	6	-6	-2	-4	-4	-2	-6	-8	0
41	4	-2	-2	4	0	2	-6	-2	-2	-4	8	6	6	-12	0
42	-2	2	0	-2	-4	4	2	4	-2	-2	0	6	-8	4	-2
43	-10	-2	-4	2	8	4	2	-8	2	6	0	-2	0	0	2
44	-6	4	-2	0	-2	-4	-14	0	-2	0	6	0	2	0	2
45	-2	0	-2	4	-2	-4	-2	-8	2	-4	-2	4	-6	8	-2
46	0	0	4	2	-10	-2	-2	-10	2	2	2	0	0	0	-4
47	8	-4	0	-2	10	-2	-2	-2	10	6	-2	-4	-4	0	4
48	-4	0	4	0	4	0	4	0	4	0	-4	0	-12	0	4
49	4	0	-4	0	4	0	4	0	4	0	-4	0	-4	0	-4
50	-6	-4	-6	2	4	2	0	-2	0	2	0	0	2	8	-2
51	6	4	6	2	0	2	4	-2	4	2	-4	0	6	0	2
52	-2	-10	0	-4	-2	2	0	2	0	-4	-2	10	-4	-4	2
53	6	-2	0	-4	-2	2	0	6	4	0	2	6	0	0	-2
54	4	6	2	2	-6	4	4	-4	0	6	2	2	-6	0	0
55	0	6	6	-6	-2	-4	0	0	8	-6	2	6	2	4	0
56	8	10	-2	0	8	2	-2	-6	6	-4	4	6	2	0	0
57	4	-2	-2	-4	0	-6	2	6	-2	-4	0	-2	6	4	0
58	-10	10	0	6	-4	4	2	-4	-2	6	0	-2	0	-4	-2
59	6	-2	-4	2	0	4	2	-8	-6	-2	0	6	0	0	2
60	2	0	2	-4	-6	4	2	4	2	8	-2	0	2	4	-2
61	-2	12	-6	8	2	-4	6	4	-2	-4	-2	4	2	-4	2
62	-8	4	0	-2	2	-2	6	10	6	2	2	0	0	-4	0
63	-8	0	4	2	-2	-10	-2	-6	6	-2	6	-4	4	-4	0

Annex B-8: The table of $NS_8(\alpha, \beta) - 32$.

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	$P_H[15] \oplus P_L[\alpha,\beta] \oplus C_H[15] \oplus C_L[\alpha,\beta]$ $= K_1[\gamma] \oplus K_2[22] \oplus L_4 \oplus L_8 \oplus K_{12}[22] \oplus K_{13}[\gamma]$	$1/2 + 1.49 \times 2^{-19}$	`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`

Notations:

`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 C: The best expression and the best probability of DES.

Annex D: A known-plaintext attack of 16-round DES using equation (25).

We here present another example of a known-plaintext attack of 16-round DES using equation (25) faster than an exhaustive key search . Refer to chapter 6 for the detailed discussions.

According to Figure 8, we have the following expression of 16-round DES which holds with probability $1/2 + 2^6(-3/64)^7 = 1/2 - 1.07 \times 2^{-25}$:

$$\begin{aligned} & P_H[0,5,10,11,20,25,27] \oplus C_L[0,5,10,11,20,25,27] \oplus \\ & \quad F_1(P_L, K_1)[0,5,10,11,20,25,27] \\ & = K_3[4,5,6,7] \oplus K_5[4,5,6,7] \oplus K_7[4,5,6,7] \oplus \\ & \quad K_9[4,5,6,7] \oplus K_{11}[4,5,6,7] \oplus K_{13}[4,5,6,7] \oplus K_{15}[4,5,6,7]. \end{aligned} \tag{45}$$

The effective text bits and the effective key bits of equation (45) are as follows:

- Effective text bits (11 bits): $P_L[0] \sim P_L[8]$, $P_L[31]$, $P_H[0,5,10,11,20,25,27] \oplus C_L[0,5,10,11,20,25,27]$,
- Effective key bits (12 bits): $K_1[0] \sim K_1[11]$.

We can hence apply Algorithm 2 to equation (45) with $2^{12} + 2^{11} = 1.5 \times 2^{12}$ counters and derive 13 subkey bits consisting of the 12 effective key bits and one subkey bit of the right side. Moreover, according to round symmetry of DES, we have another expression of 16-round DES which holds with the same probability as equation (45):

$$\begin{aligned} & C_H[0,5,10,11,20,25,27] \oplus P_L[0,5,10,11,20,25,27] \oplus \\ & \quad F_{16}(C_L, K_{16})[0,5,10,11,20,25,27] \\ & = K_{14}[4,5,6,7] \oplus K_{12}[4,5,6,7] \oplus K_{10}[4,5,6,7] \oplus \\ & \quad K_8[4,5,6,7] \oplus K_6[4,5,6,7] \oplus K_4[4,5,6,7] \oplus K_2[4,5,6,7]. \end{aligned} \tag{46}$$

The solution of equation (46) gives us another 13 subkey bits; namely, $K_{16}[0] \sim K_{16}[11]$ and the right side of equation (46). In this stage, we have 26 subkey bits, which correspond to 24 secret key bits since 2 subkey bits are duplicate. The remaining 32 secret key bits are now easily derived by an exhaustive search. According to the discussion similar to chapter 6, we can see that this attack is expected to be successful when $8|1.07 \times 2^{-25}|^{-2} = 1.75 \times 2^{52}$ random known-plaintexts are available. This concludes that our attack is also faster than an exhaustive key search.

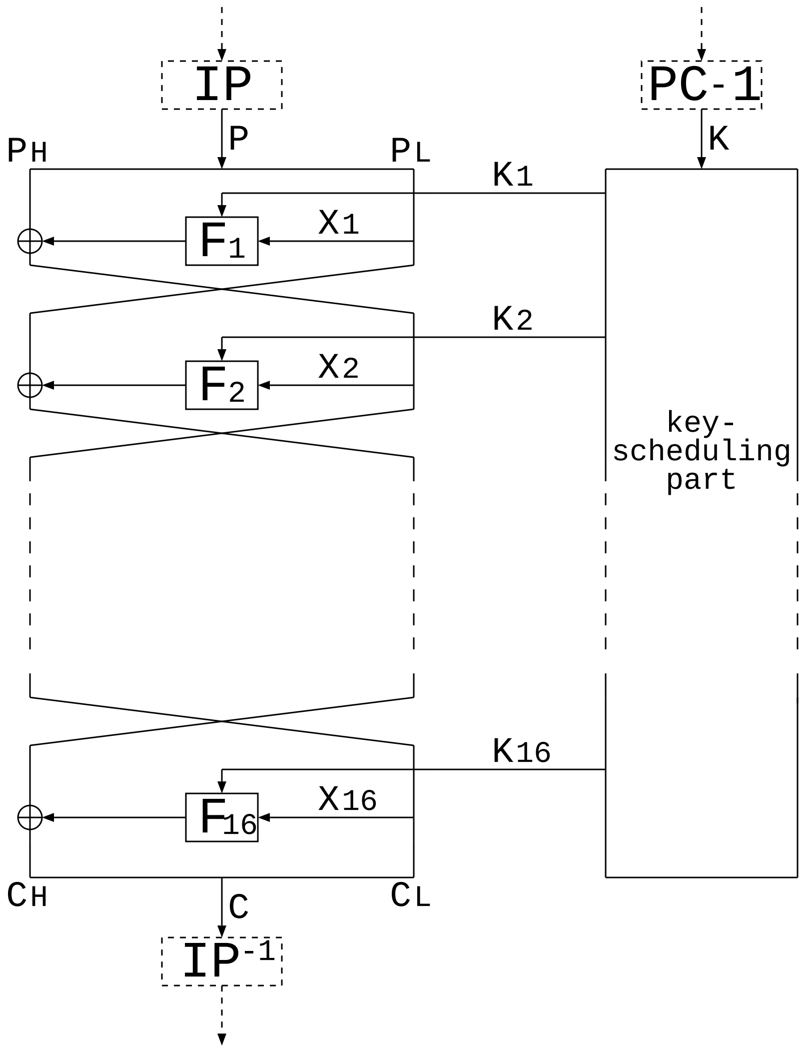

Figure 1: DES cipher.

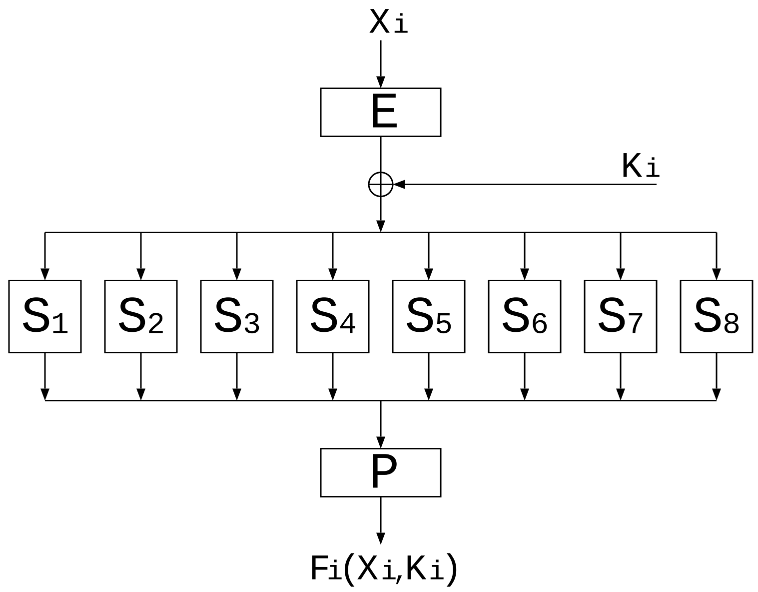

Figure 2: The F-function.

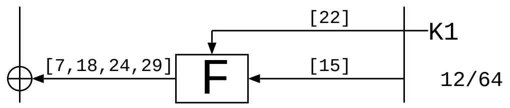

Figure 3: The best linear approximation of F-function.

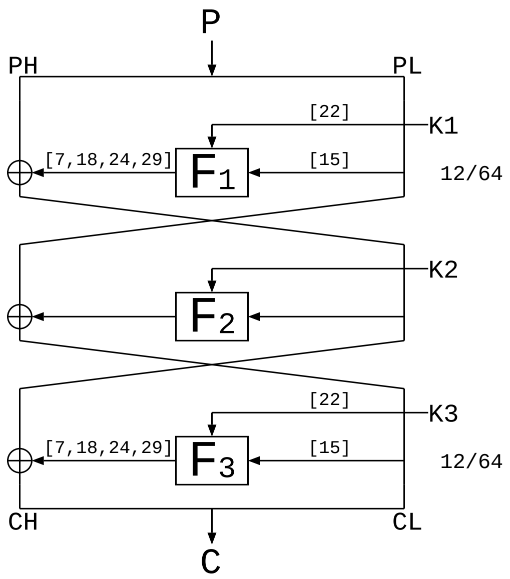

Figure 4: The best linear approximation of 3-round DES.

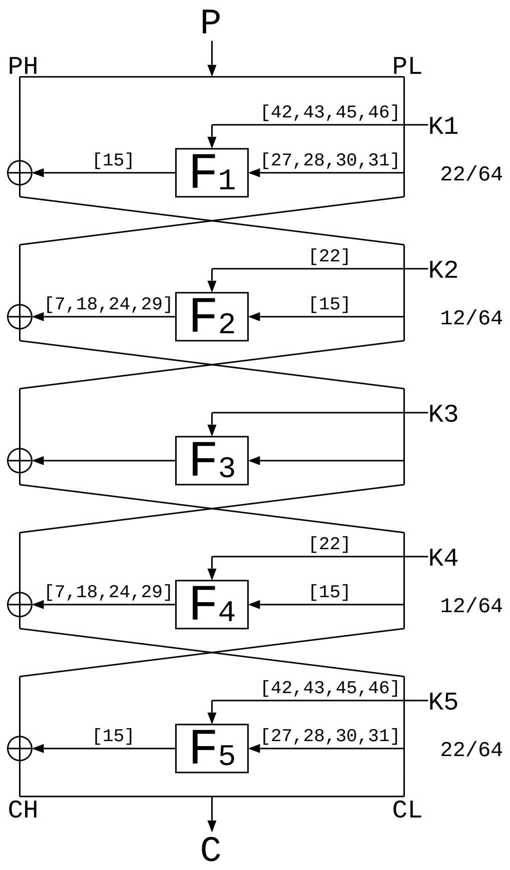

Figure 5: The best linear approximation of 5-round DES.

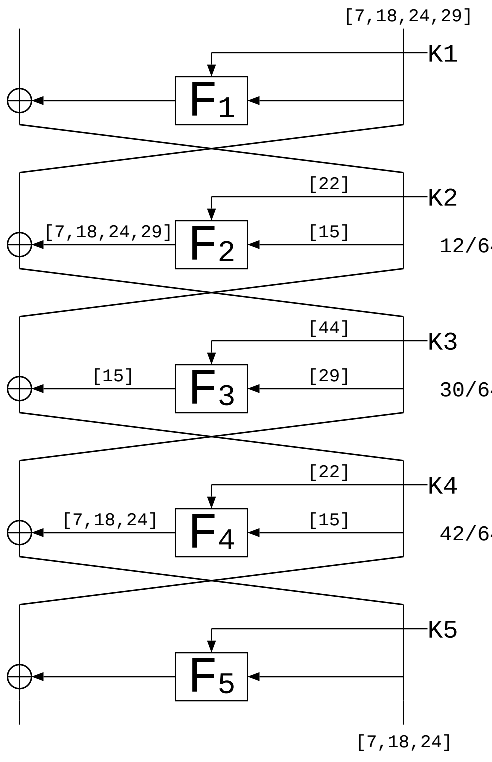

Figure 6: Another 5-round linear approximation.

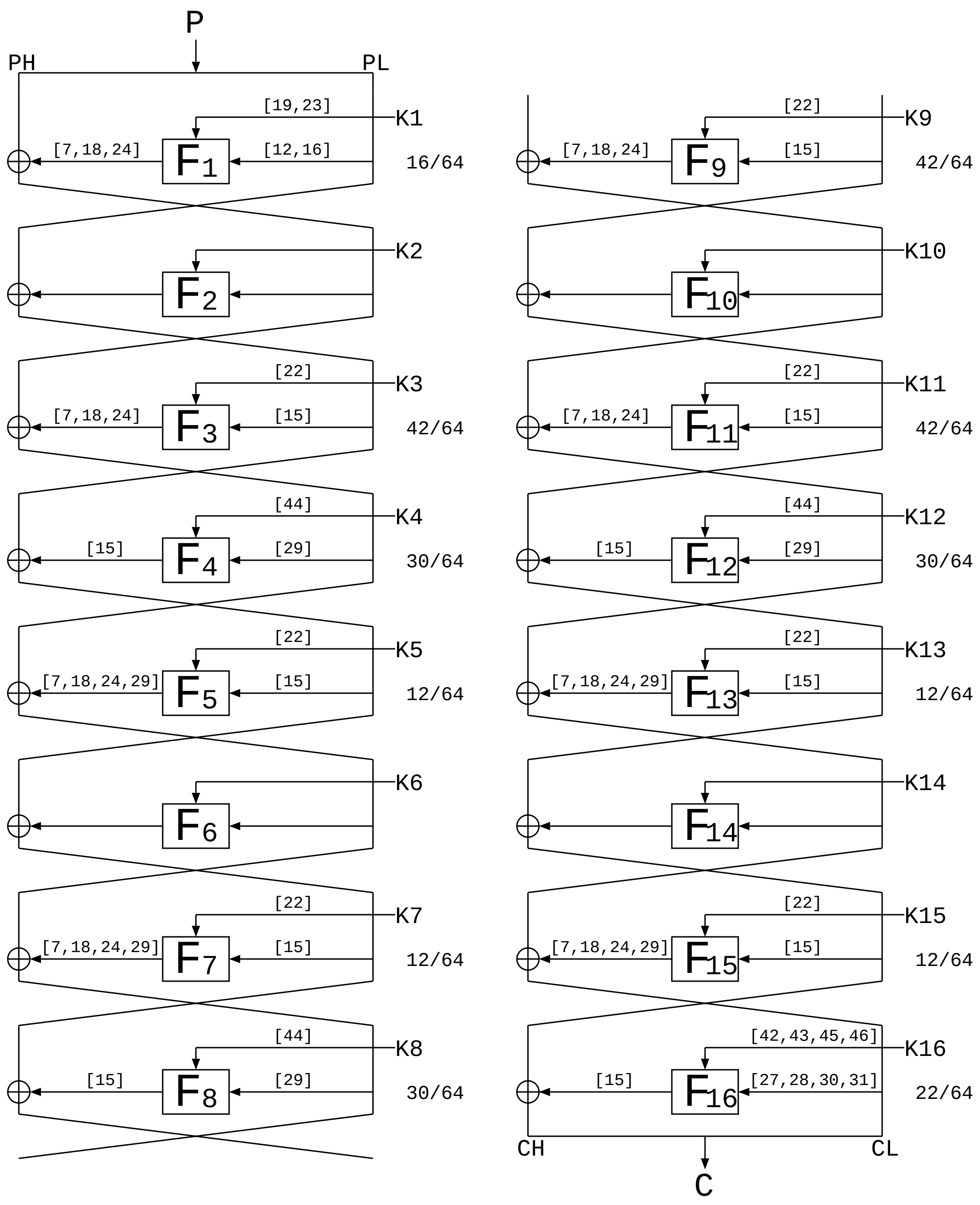

Figure 7: The best linear approximation of 16-round DES.

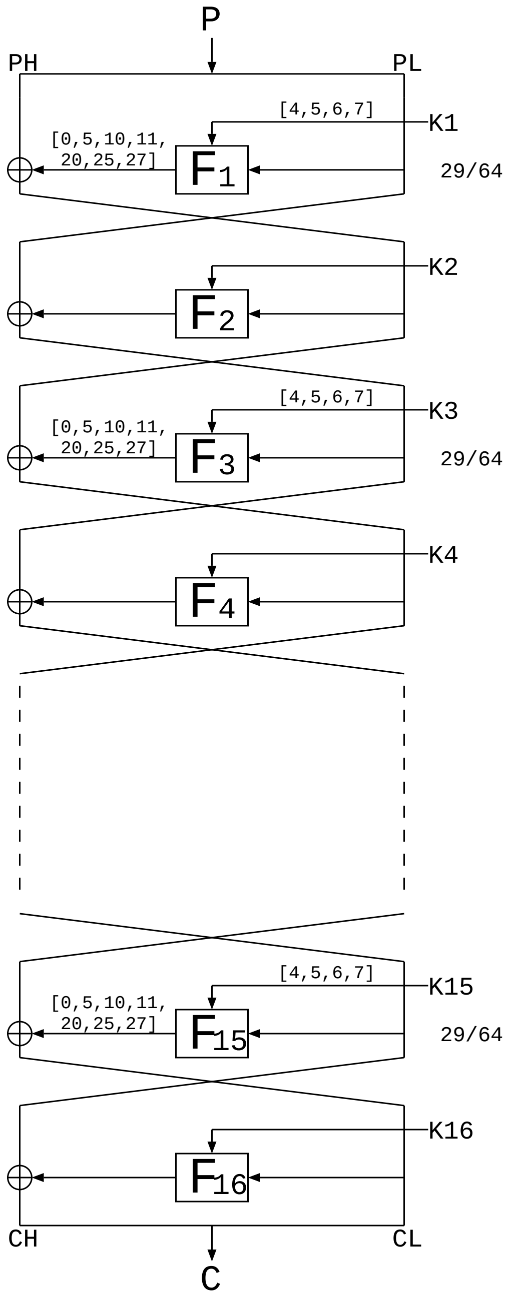

Figure 8: Another linear approximation of 16-round DES.

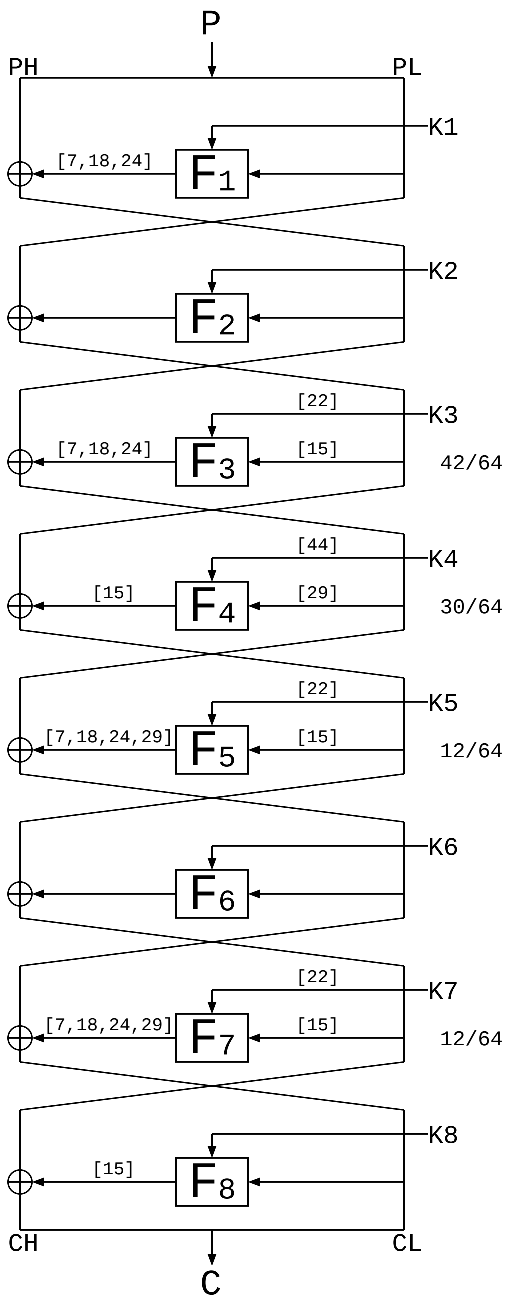

Figure 9: The known-plaintext attack of 8-round DES (I).

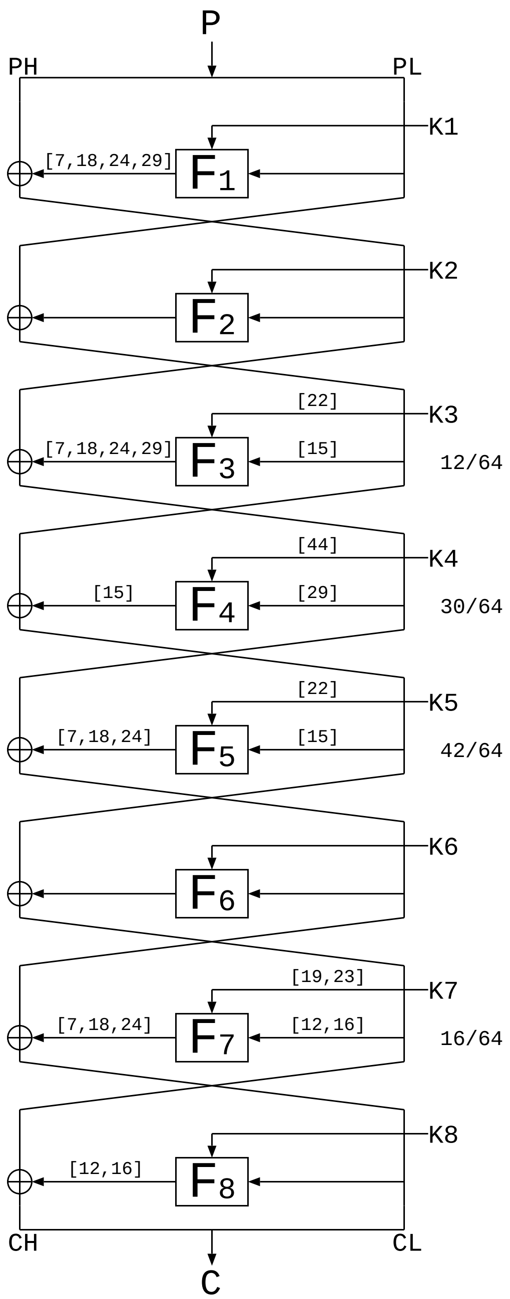

Figure 10: The known-plaintext attack of 8-round DES (II).

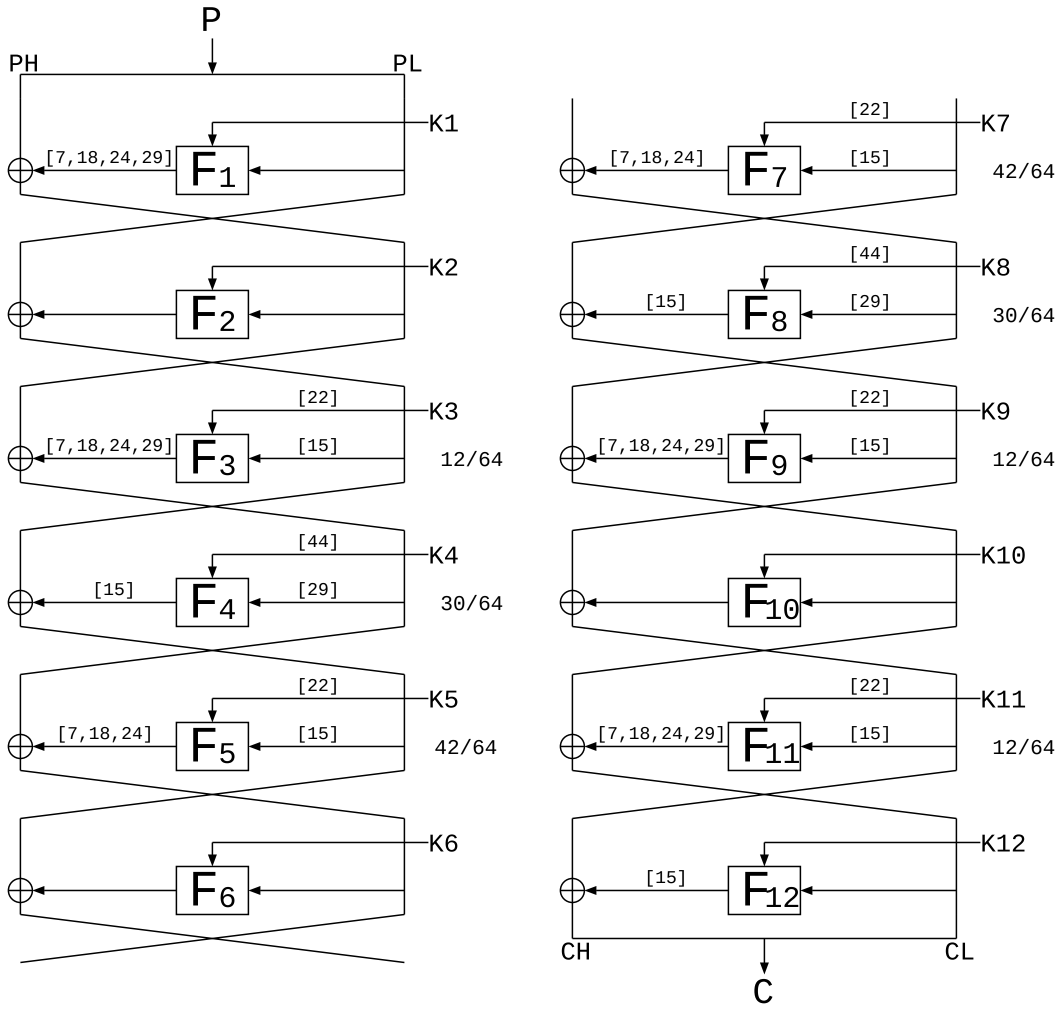

Figure 11: The known-plaintext attack of 12-round DES.

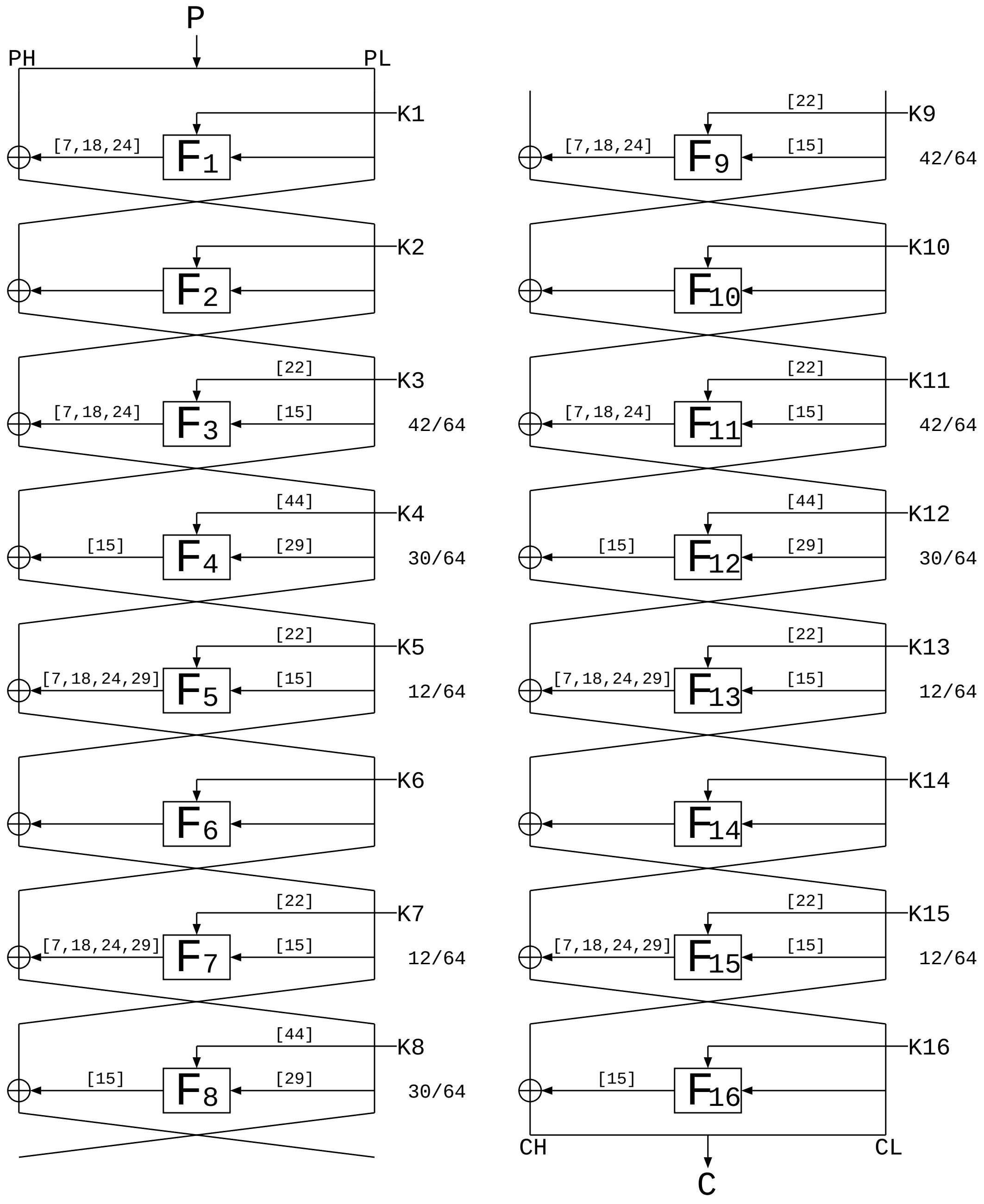

Figure 12: The known-plaintext attack of 16-round DES.