A New Method for Known Plaintext Attack of FEAL Cipher

Mitsuru Matsui Atsuhiro Yamagishi

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 propose a new known plaintext attack of FEAL cipher. Our method differs from previous statistical ones in point of deriving the extended key in definite way. As a result, it is possible to break FEAL-4 with 5 known plaintexts and FEAL-6 with 100 known plaintexts respectively. Moreover, we show a method to break FEAL-8 with 2^{15} known plaintexts faster than an exhaustive search.

1 Introduction

FEAL cipher [SM, MKOM] is a block cipher algorithm which is designed for software implementations on 8 or 16 bit microprocessors. The most recent version of FEAL cipher is announced as FEAL-NX, where N is the number of rounds and X denotes an optional 128 bit key input.

As for known plaintext attacks of FEAL cipher, Biham and Shamir have shown FEAL-8 is breakable with 2^{38} known plaintexts using differential cryptanalysis [BS], and Tardy-Corfdir and Gilbert have presented a statistical method to break FEAL-4 with 1000 known plaintexts and FEAL-6 with 20000 known plaintexts respectively [TG].

In this paper, we propose a new technique of a known plaintext attack of FEAL cipher. Our method is a kind of meet-in-the-middle attack with a partial exhaustive search; hence we can derive the extended key directly and definitely. We have made

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 81-91, 1993.

computer experiments to attack FEAL cipher with up to seven rounds. As for FEAL-8, we have estimated the computational complexity to derive the key.

The main results in this paper are as follows. The experiments were implemented with C and assembly language programs on HP9425 workstation computer (68040/25MHz).

- FEAL-4 is breakable with 5 known plaintexts in 6 minutes.
- FEAL-6 is breakable with 100 known plaintexts in 40 minutes.
- FEAL-7 is breakable with 2^{14} known plaintexts in 170 hours.
- FEAL-8 is breakable with 2^{15} known plaintexts faster than an exhaustive search for 64-bit keys and with 2^{28} known plaintexts as fast as an exhaustive search for 50-bit keys.

2 Preliminaries

We use the following notations throughout this paper.

P : The plain text.
C : The corresponding cipher text.
P_H, C_H : The left 32 bit data of P and C respectively.
P_L, C_L : The right 32 bit data of P and C respectively.
$A[i]$: The i-th bit of A.
$A[i, j, ..., k]$: The XORed value of the i-th, j-th,.., and k-th bits of A.
$A[i \sim j]$: The $j - i + 1$ bit data consisting of the i-th, i+1-th,.., and j-th bits of A.

For convenience of the following chapters, we define modified F-function $O_R = mF_R(I_R, K_R)$ as figure 1, where R denotes the round.

Then one has easily

$$I[0] = O[2, 8] \oplus K[0], \tag{1}$$
$$I[8] = O[2, 8, 10, 16] \oplus K[0, 8], \tag{2}$$
$$I[16] = O[10, 18, 26] \oplus K[16, 24], \tag{3}$$
$$I[24] = O[16, 26] \oplus K[24]. \tag{4}$$

Consequently, for three round algorithm with modified F-function as figure 2, we obtain the following useful relations which hold for any plaintext P and the corresponding ciphertext C by tracing the bold line in figure 2:

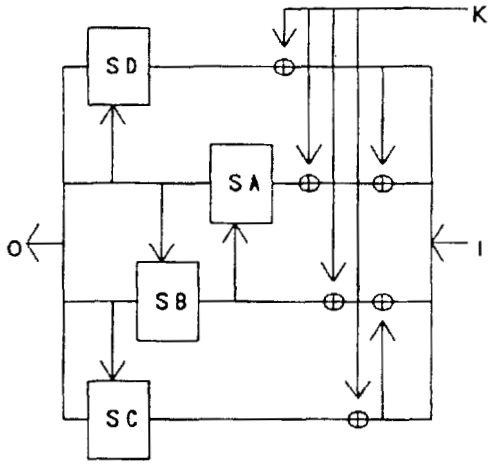
$$P_H[2,8] \oplus P_L[0] \oplus C_H[2,8] \oplus C_L[0] = K_1[0] \oplus K_3[0] \oplus K_4[2,8], \tag{5}$$

$$P_H[2,8,10,16] \oplus P_L[8] \oplus C_H[2,8,10,16] \oplus C_L[8] = K_1[0,8] \oplus K_3[0,8] \oplus K_4[2,8,10,16], \tag{6}$$

$$P_H[10,18,26] \oplus P_L[16] \oplus C_H[10,18,26] \oplus C_L[16] = K_1[16,24] \oplus K_3[16,24] \oplus K_4[10,18,26], \tag{7}$$

$$P_H[16,26] \oplus P_L[24] \oplus C_H[16,26] \oplus C_L[24] = K_1[24] \oplus K_3[24] \oplus K_4[16,26]. \tag{8}$$

We note that the left side of each equation is a constant value for an attacker. In the following chapters, we will construct similar constant functions for each cipher so that the number of related key bits is as small as possible.



S A(x, y) = S C(x, y) = ROL2(x+y+1(mod256))
S B(x, y) = S D(x, y) = ROL2(x+y(mod256))

Figure 1 : Modified F function

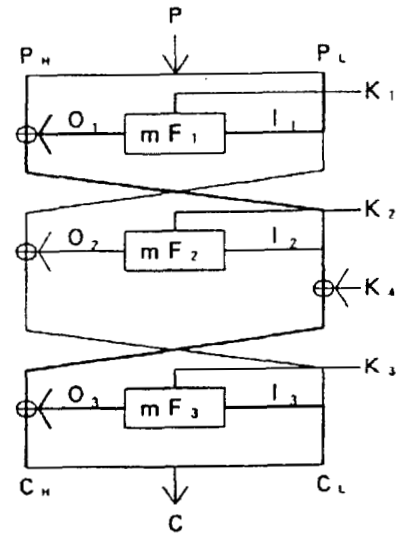


Figure 2 : Three round algorithm

3 Principle of the attack

First, we construct explicitly a function $g(x, y, z)$ which satisfies the following conditions:

- The size of z is sufficiently small.
- There exists $\tilde{K}$ which depends only on the extended key, then $g(P, C, \tilde{K})$ is a constant value for any plaintext P and the corresponding ciphertext C.
- For any fixed $K \neq \tilde{K}$, there exist plaintexts P, P' and the corresponding ciphertexts C, C' such that $g(P, C, K) \neq g(P', C', K)$.

Once we succeed in obtaining g, then we are able to make an exhaustive search for $\tilde{K}$; namely, for all possible K we verify that g always outputs a constant value for given known plaintexts and the corresponding ciphertexts. Since this verification is expected to fail in almost cases except the correct $\tilde{K}$, we will obtain only several candidates for $\tilde{K}$ if we have sufficiently many known plaintexts. By repeating this method using various functions, we can reach whole key bits finally.

Although this attack is effective when the number of rounds is small, it is generally difficult to find a function g so that the size of z is sufficiently small. Then next, we try to reduce the substantial size of z in g by selecting convenient plaintexts to attack. This is realized by controlling the spread of carry bits of the addition in S-boxes.

Our method determines the extended key directly and definitely, moreover the computational complexity generally decreases as the number of known plaintexts increases. In subsequent chapters we will describe the results of our computer experiments about the number of known plaintexts and the breaking time for each cipher with the independent extended key bits.

4 Attack of FEAL-4

We start to rewrite FEAL-4 as figure 3. Then the original extended key is corresponding to $K_1, K_2, .., K_6$ in figure 3 one-to-one and linearly. Hence in this chapter we describe the method to derive these keys from given known plaintexts.

First, applying the equation (7) from the second round to the fourth round in figure 3, we obtain

$$P_H[10, 16, 18, 26] \oplus P_L[10, 18, 26] \oplus C_H[10, 16, 18, 26] \oplus C_L[16] \oplus mF_1(P_H \oplus P_L, K_1)[16] = T, \tag{9}$$

where T is independent of P and C.

Now we can easily see that the key bits which influence the left side of the equation (9) are $K_1[8 \sim 14]$ and $K_1[16 \sim 22]$, in which $K_1[14]$ and $K_1[22]$ are only XORed in the left side. Hence by transposing these two bits to the right side, we may suppose the essential key bits in the left side are $K_1[8 \sim 13]$ and $K_1[16 \sim 21]$. We call these bits the effective key bits in the equation (9).

Therefore, we obtain candidates for $K_1[8 \sim 13]$ and $K_1[16 \sim 21]$ through an exhaustive search for 12-bit keys by checking that the left side of the equation (9) gives a constant value for every known plaintext and the corresponding ciphertext.

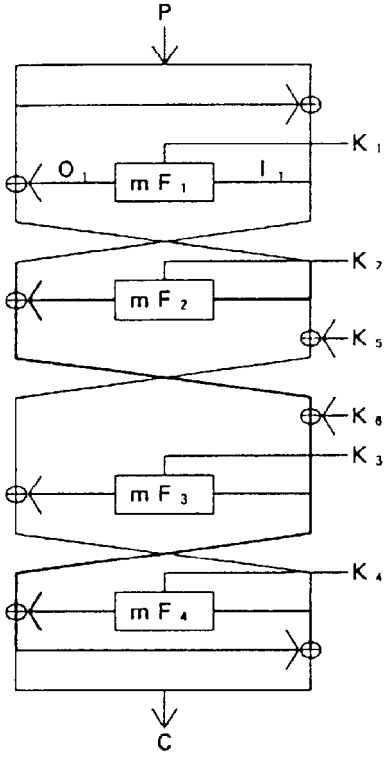


Figure 3: FEAL-4 cipher

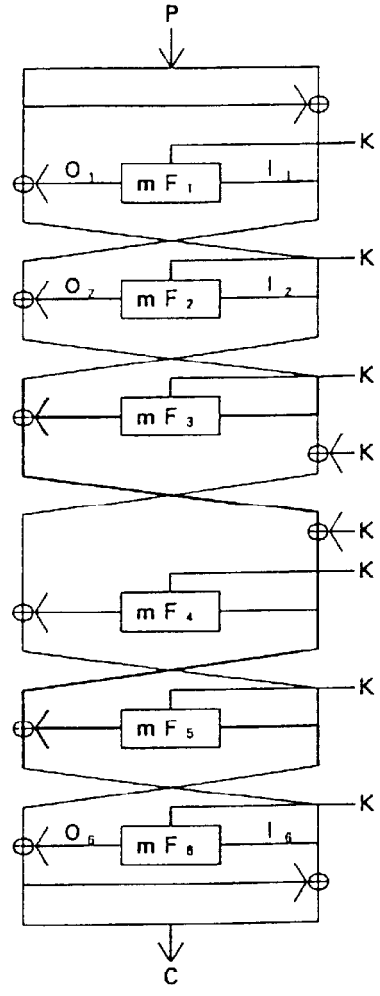


Figure 4: FEAL-6 cipher

Similarly applying the equations (6), (8) and (9) in figure 3, one has candidates for $K_1[0 \sim 5]$ and $K_1[8 \sim 29]$ finally. It is easy to derive remaining bits, so we omit the detail.

In our computer experiments to derive $K_1, K_2, .., K_6$ completely, it takes 2 seconds with 10 known plaintexts and 350 seconds with 5 known plaintexts respectively. Our program uses 30KB memory in running.

5 Attack of FEAL-6

We also start to rewrite FEAL-6 as figure 4. In this case $K_1, K_2, .., K_8$ are not independent; for example we may suppose

$$\begin{aligned} &K_1[j] = K_3[j], \\ &K_4[j] = K_6[j] \quad (0 \le j \le 7\ ,\ 24 \le j \le 31), \end{aligned} \tag{10}$$

though we do not need these relations afterward.

Now applying the equation (7) from the third round to the fifth round in figure 4, we obtain

$$\begin{aligned} &P_H[10, 18, 26] \oplus C_H[10, 16, 18, 26] \oplus C_L[10, 18, 26] \oplus \\ &mF_2(P_H \oplus mF_1(P_H \oplus P_L, K_1), K_2)[16] \oplus \\ &mF_6(C_H \oplus C_L, K_6)[16] = T. \end{aligned} \tag{11}$$

Then we easily see that the effective key bits in the equation (11) are the following 48 bits:

$$K_1[0 \sim 3], K_1[8 \sim 27], K_i[8 \sim 13], K_i[16 \sim 21] \quad (i = 2, 6). \tag{12}$$

However, it is computationally heavy to solve this equation using the same search method as FEAL-4. Hence we try to reduce the number of the effective key bits. First assume

$$I_6[5, 13, 21, 29] \oplus K_6[13, 21] = 0, \tag{13}$$

then the carry bit from the 5-th to the 6-th bit in the addition of S-box S_A in mF_6 can be denoted as

$$I_6[5, 13] \oplus K_6[13]. \tag{14}$$

This shows we may ignore the influence of $K_6[8 \sim 12]$ and $K_6[16 \sim 20]$ in the left side of the equation (11) under the assumption (13). Similarly assuming

$$I_2[5, 13, 21, 29] \oplus K_2[13, 21] = 0, \tag{15}$$

we can eliminate the influence of $K_2[8 \sim 12]$ and $K_2[16 \sim 20]$, and hence the effective key bits in the equation (11) are reduced to the following 26 bits:

$$K_1[0 \sim 3], K_1[8 \sim 27], K_2[13, 21], K_6[13, 21]. \tag{16}$$

In fact the following search algorithm leads us to obtain candidates for these bits.

Step 1 Select 26-bit data $K_1[0 \sim 3], K_1[8 \sim 27], K_2[13, 21], K_6[13, 21]$.

Step 2 Calculate I_2 and I_6 from given plaintexts and the corresponding ciphertexts.

Step 3 Check that the left side of the equation (11) gives a constant value for every plaintext which satisfies the equations (13) and (15).

Step 4 If the check is correct, then let the 26-bit data be a candidate. Otherwise, the selection in step 1 is wrong.

Subsequently, we can reach other key bits using a similar method to breaking FEAL-4, however we omit the detail. In our computer experiments using randomly generated 100 known plaintexts, it takes 37 minutes to derive $K_1, K_2, .., K_8$ completely. Our program uses 100KB memory in running.

Moreover, we can solve the key faster by adding more relations and known plaintexts. For example, assume

$$I_1[5, 13, 21, 29] \oplus K_1[13, 21] = 0, \tag{17}$$

$$I_1[0, 8, 16, 24, 26] \oplus K_1[8, 16, 26] = 1, \tag{18}$$

$$I_1[6, 14, 22, 30] \oplus K_1[14, 22] = 0, \tag{19}$$

$$I_1[0, 2, 5, 6, 8, 13, 14, 22, 30] \oplus K_1[2, 8, 13, 14, 22] = 0, \tag{20}$$

which are introduced in order to cut off the spread of each carry bit at the 5-th bit of S_A, the 2-nd bit of S_C, the 6-th bit of S_A and the 2-nd bit of S_D in mF_1 respectively. Then the effective key bits in the equation (11) are reduced to the following 18 bits:

$$K_1[2 \sim 3], K_1[8 \sim 11], K_1[13], K_1[14, 22], K_1[15, 22, 23],$$
$$K_1[16 \sim 19], K_1[21], K_1[26 \sim 27], K_2[13, 21], K_6[13, 21]. \tag{21}$$

After the calculation of these 18 bits, we can reach whole 26 bits by repeating the previous method without equations (17) $\sim$ (20). In this case, the derivation of $K_1, K_2, .., K_8$ takes 5 minutes using 500 known plaintexts and 32 minutes using 200 known plaintexts respectively.

6 Attack of FEAL-7

The principle of breaking FEAL-7 is the same as FEAL-6. Now our fundamental equation is

$$\begin{aligned} &mF_2(P_H \oplus mF_1(P_H \oplus P_L, K_1), K_2)[16] \oplus \\ &mF_6(C_H \oplus mF_7(C_H \oplus C_L, K_7), K_6)[16] \oplus \\ &P_H[10, 18, 26] \oplus C_H[10, 18, 26] = T. \end{aligned} \tag{22}$$

In this case we use known plaintexts which satisfy (13),(15),(17) $\sim$ (20) and subsequent four relations simultaneously:

$$I_7[5, 13, 21, 29] \oplus K_7[13, 21] = 0, \tag{23}$$

$$I_7[0, 8, 16, 24, 26] \oplus K_7[8, 16, 26] = 1, \tag{24}$$

$$I_7[6, 14, 22, 30] \oplus K_7[14, 22] = 0, \tag{25}$$

$$I_7[0, 2, 5, 6, 8, 13, 14, 22, 30] \oplus K_7[2, 8, 13, 14, 22] = 0. \tag{26}$$

Then the effective key bits in the equation (22) are the following 34 bits:

$$\begin{aligned} &K_i[2 \sim 3], K_i[8 \sim 11], K_i[13], K_i[14, 22], K_i[15, 22, 23], \\ &K_i[16 \sim 19], K_i[21], K_i[26 \sim 27], K_2[13, 21], K_6[13, 21] \quad (i = 1, 7). \end{aligned} \tag{27}$$

We have described a FEAL-7 breaking program to derive the extended key with 2^{14} randomly generated known plaintexts. This program uses 700KB memory in executing. It takes 170 hours to complete our attack.

7 Attack of FEAL-8

Our algorithm to attack FEAL-8 with independent keys $K_1, K_2, .., K_{10}$ (figure 5) is to decipher by one round using K_8, and then to apply the attack of FEAL-7. Since this computation is beyond our computer's power, in this chapter we try to estimate the computational complexity of our attack.

First, we note the choices of K_8 are 2^{30} since $K_8[7]$ and $K_8[31]$ are only XORed in mF_8. Hence these 2 bits may be included in other key bits. For example, we may modify the keys as follows:

$$\begin{aligned} &K_i[1] = K_i[1] \oplus K_8[7] \quad (i = 5, 7, 10), \\ &K_i[9] = K_i[9] \oplus K_8[7] \quad (i = 5, 7), \\ &K_i[17] = K_i[17] \oplus K_8[31] \quad (i = 5, 7), \\ &K_i[25] = K_i[25] \oplus K_8[31] \quad (i = 5, 7, 10), \\ &K_8[7] = K_8[31] = 0. \end{aligned} \tag{28}$$

Consequently, the total time required to break FEAL-8 is estimated to be 2^{30} times as much time as FEAL-7.

Next, we have constructed a simple key search program of FEAL-8 using assembly language in order to compare our method with exhaustive key search. As a result, the breaking time of FEAL-7 using our method is almost same as exhaustive search for 34-bit keys of FEAL-8. This shows the computational time to attack FEAL-8 with 2^{14} known plaintexts is estimated to be the same as exhaustive search for 64-bit keys.

For the rest of this chapter, we try to reduce the computational complexity. Now assume

$$O_8[16] = 0. \tag{29}$$

Then we note $K_8[24]$ can be also included in other key bits. Namely, we may modify the key as follows:

$$\begin{aligned} &K_i[18] = K_i[18] \oplus K_8[24] \quad (i = 5, 7), \\ &K_i[26] = K_i[26] \oplus K_8[24] \quad (i = 5, 7, 10), \\ &K_8[24] = 0. \end{aligned} \tag{30}$$

This reduces the choices for K_8 to 2^{29}. Nevertheless, since the ciphertexts which satisfy the equation (29) are half of whole ones, we need twice as many known plaintexts to attack FEAL-7 with the same efficiency.

This fact also holds on $O_8[17]$,$O_8[18]$,..,$O_8[22]$ and $O_8[8]$,$O_8[9]$,..,$O_8[14]$ in this order. Namely, by assuming the equations

$$\begin{aligned} &O_8[i] = 0 \quad (17 \le i \le 22), \\ &O_8[i] = 1 \quad (8 \le i \le 14), \end{aligned} \tag{31}$$

we can reduce 13 more bits for key search, though we need 2^{13} times as many plaintexts. Then similar key modifications are possible; for example, as for $O_8[8]$ we may suppose

$$\begin{aligned} &K_i[2] = K_i[2] \oplus K_8[0] \quad (i = 5, 7, 10), \\ &K_i[10] = K_i[10] \oplus K_8[0] \quad (i = 5, 7), \\ &K_8[0] = 0. \end{aligned} \tag{32}$$

This shows the breaking time of FEAL-8 with 2^{28} known plaintexts is the same as exhaustive search for 50-bit keys. In fact, we can use the following algorithm to carry out the attack of FEAL-8:

Step 1 Select a candidate of 16-bit data $K_8[8 \sim 23]$, and then let $K_8[j] = 0$ $(0 \leq j \leq 7\ ,\ 24 \leq j \leq 31)$.

Step 2 Decipher by one round using the key K_8 and given ciphertexts.

Step 3 Attack the FEAL-7 using known plaintexts and the corresponding ciphertexts which satisfy (29) and (31).

Step 4 If $K_8[8 \sim 23]$ is the correct value, the attack of step 3 succeeds. Otherwise it fails.

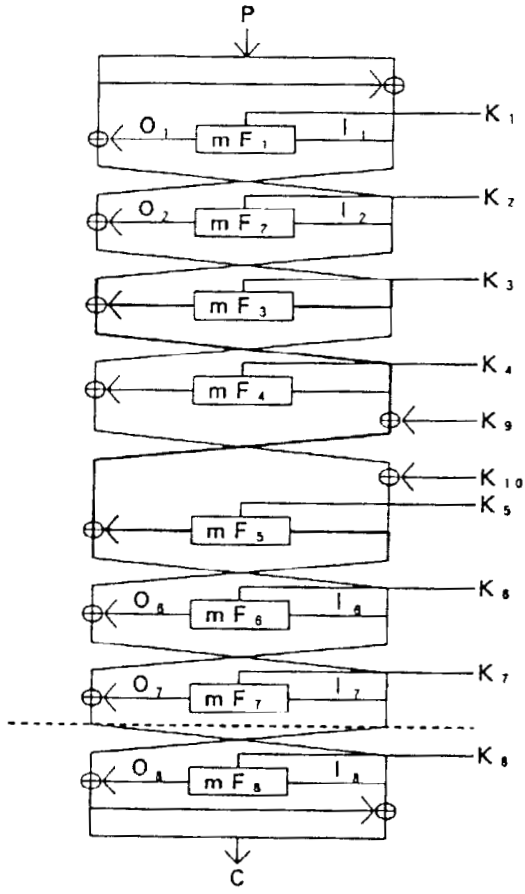


Figure 5 : FEAL-8 cipher

8 Conclusion

We have introduced a new method to attack FEAL cipher with up to eight rounds. Our attack derives the extended key directly and definitely without any assumption of the key schedule algorithm. Moreover we have proposed a method to reduce the computational time at the cost of the number of known plaintexts. As for FEAL-8, it is still possible to reduce the breaking time with more known plaintexts. We will discuss it in the full paper.

Acknowledgement

The authors would like to thank Kouichi Sakurai and Tohru Inoue very much for their many helpful comments and many hours of discussion about this work.

References

[SM] A. Shimizu and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL," *Advances in Cryptology, Proceedings of EUROCRYPT '87*, pp.267, 1987.

[MKOM] S. Miyaguchi, S. Kurihara, K. Ohta and H. Morita, "Expansion of FEAL cipher," *NTT Review Vol.2 No.6* , pp.116-127, 1990.

[BS] E. Biham and A. Shamir, "Differential Cryptanalysis of FEAL and N-Hash," *Extended Abstract, Proceedings of EUROCRYPT '91*, 1991.

[TG] A. Tardy-Corfdir and H. Gilbert, "A known plaintext attack of FEAL-4 and FEAL-6," *Proceedings of Crypto '91*, 1991.