Linear Cryptanalysis of the Fast Data Encipherment Algorithm

Kazuo Ohta[1] and Kazumaro Aoki[2*]

[1] NTT Network Information Systems Laboratories
1-2356 Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan
[2] Department of Mathematics
School of Science and Engineering, Waseda University
3-4-1 Ookubo, Shinjuku-ku, Tokyo-to, 169 Japan

Abstract. This paper discusses the security of the Fast Data Encipherment Algorithm (FEAL) against Linear Cryptanalysis. It has been confirmed that the entire subkeys used in FEAL–8 can be derived with 2^{25} pairs of known plaintexts and ciphertexts with a success rate approximately 70% spending about 1 hour using a WS (SPARCstation 10 Model 30). This paper also evaluates the security of FEAL–N in comparison with that of the Data Encryption Standard (DES).

1 Introduction

This paper analyzes the applicability of Linear Cryptanalysis to the Fast Data Encipherment Algorithm (FEAL) [MSS88]. The structure of FEAL is similar to DES, except, for example, the permutation and the S-Boxes in F-function of DES are replaced by byte rotation and addition operation, and these differences are interesting from the viewpoint of cryptanalysis. In the Linear Cryptanalysis of FEAL, our main concerns in evaluating the security of FEAL considering the replacement of F-function and S-Boxes are: 1) how to find effective linear expressions, 2) an estimation of the success rate against the number of pairs of plaintexts and corresponding ciphertexts and the approximate probability, and 3) an estimation of the memory size and the processing amount of the attack.

2 Linear Cryptanalysis

2.1 Notations and Preliminaries

The modified FEAL and its modified F-function [MY92] are analyzed here. We use the similar notations and define the right most bit of each symbol as the 0-th bit, which is the lowest bit, as well as in the reference [M93].

2.2 Principle

Linear Cryptanalysis analyzes the probability that the following equation holds.

$$P[i_1, i_2, \ldots, i_a] \oplus C[j_1, j_2, \ldots, j_b] = S[k_1, k_2 \ldots, k_c], \qquad (1)$$

where $i_1, i_2, \ldots, i_a, j_1, j_2, \ldots, j_b, k_1, k_2 \ldots, k_c$ are fixed bit locations defined by the linear expression, $(\Gamma P, \Gamma C, \Gamma K)$. The value of the right side of this equation depends only on the key values. We denote $S[k_1, k_2 \ldots, k_c]$ by S simply.

[*] A part of this research was conducted while the second author stayed at NTT Network Information Systems Laboratories as a spring intern in March of 1994.

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 12-16, 1994.

Two kinds of probability are defined in Linear Cryptanalysis: one is $p = \text{Prob}_{P,K}\{E(P,K)(\Gamma C) \oplus P(\Gamma P) = K(\Gamma K)\}$, and the other is the absolute value of probability different from a half, $p' = |p - 1/2|$. Hereafter, p' will be used as the *probability* of the linear expression $(\Gamma P, \Gamma C, \Gamma K)$.

2.3 Implementation Techniques

Matsui [M93] proposed the following practical implementation of an attack against DES, and captured the *effective text bits* among text information, P and C, which are essential to calculate Equation (2), and the *effective key bits* among key information, K_1 and K_n, which are essential to calculate Equation (2). Hereafter, t and k denote the number of effective text bits and the number of effective key bits, respectively.

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

Algorithm 1 (Counter Technique)

Step 1: Prepare 2^t counters $U_i (0 \le i < 2^t)$, where i corresponds to each value on the t effective text bits of Equation (2).

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

Step 3: Prepare 2^k counters $T_j (0 \le j < 2^k)$, where j corresponds to each value on the k effective text bits of Equation (2).

Step 4: For each 'j' of **Step 3**, let T_j be the sum of U_i's such that the left side of Equation (2), whose value can be uniquely determined by i and j, is equal to 0.

Step 5: Let $T_{max}(T_{min})$ be the maximal(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 $S = 0$ 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 $S = 1$ when $p > 1/2$ or 0 when $p < 1/2$.

The computational complexity of this procedure is $O(N) + O(2^{t+k})$. The number of counters, U_i and T_j, required by this procedure is $2^t + 2^k$. If we approximate $(n-2)$-round F-functions from the second round to the $(n-1)$-th round based on an $(n-2)$-round linear expression, we call this strategy **2-Round Elimination**. **1-Round Elimination** is also defined using an $(n-1)$-round linear expression.

3 Linear Approximation of FEAL

3.1 What are the Problems

The essential differences between DES and FEAL are the structure of S-Boxes and that of F-function. More exactly, S-Boxes of DES are defined in a non-mathematical way using tables. S-Boxes of FEAL are defined mathematically using modular addition calculation with two bits left rotation. So it seems easier to find some property of S-Boxes of FEAL than that of DES. On the other hand, the eight S-Boxes in F-function of DES act in parallel more independently than four S-Boxes in F-function of FEAL which act sequentially, where the byte rotation is built in instead of the permutation of DES. Thus, it seems easier to find some semi-global property of F-function of DES than that of FEAL.

3.2 Linear Expressions of F-function

We get various linear expressions of S-Boxes approximating the addition operation with the bitwise consideration of carry propagation as was done in [CG91].

When $a + b = x$, for example, $a[i] \oplus b[i] = x[i]$ holds with probability of $2^{-(i+1)}(i \geq 0)$, $a[i, i-j] \oplus b[i] = x[i]$, $a[i] \oplus b[i, i-j] = x[i]$ and $a[i] \oplus b[i] = x[i, i-j]$ hold with probability of $2^{-(j+1)}(1 \leq j \leq i)$. Note that $a[0] \oplus b[0] = x[0]$ always holds, since there is no carry at the least significant bit in the addition operation, and this gives 15 non-trivial linear expressions of F-function with probability of 1/2, which can be always extended to 3-round linear expressions. If $j = 1$, we can make many examples with probability of 1/4 ignoring the bit position of i. This gives many local linear expressions with probability of 1/4.

Here the concatenation rule of operations inside the F-function [B94, M94] is also applicable in the same way as that between F-functions.

3.3 Linear Expressions of Reduced Round FEAL

We developed the following search algorithm to find effective 7-round linear expressions, where $(\Gamma Y_{4-r}, \Gamma X_{4-r}) = (\Gamma Y_{4+r}, \Gamma X_{4+r})$ holds for $r = 1, 2, 3$.

Algorithm 2 (Search Algorithm of 7-Round Linear Expression)

Step 1: Set $(\Gamma Y_4, \Gamma X_4) = (0, 0)$.

Step 2: Select $(\Gamma Y_2, \Gamma X_2)$ of F-function whose probability is 1/2.

Step 3: Search ΓY_3 where $(\Gamma Y_3, \Gamma X_3)$ has the probability of 2^{-2}, given $\Gamma X_3 = \Gamma Y_2$.

Step 4: Search $\Gamma X_2'$ where $(\Gamma X_2, \Gamma X_2')$ has the probability of greater than or equal to 2^{-3}.

Step 5: Put $(\Gamma Y_1, \Gamma X_1) = (\Gamma Y_3 \oplus \Gamma X_2, \Gamma X_3 \oplus \Gamma X_2')$. Check whether its probability is greater than or equal to 2^{-4} exhaustively, if $(\Gamma Y_3, \Gamma X_3)$ activates the same S-Boxes of F-function as $(\Gamma X_2, \Gamma X_2')$.

We have found the following eight pairs $(\Gamma X_2, \Gamma X_2')$ using the above algorithm and sixteen 7-round linear expressions with probability of greater than 2^{-9}. This is one of examples with probability of 1.764×2^{-9}, which is effective in our implementation described in Section 5.

Note that the middle 5-round part of the expression also has the probability of 1/8, while Biham described a 5-round linear expression with probability of 1/32 in [B94].

ΓX_2	$\Gamma X_2'$
00000100	10105050
00000100	18185858
00000100	10107878
00000100	18187070
01000000	50101010
01000000	58181818
01000000	70101818
01000000	78181010

r	ΓY_r	ΓX_r	p_r'	
P	1D000400	50101010		
1	1D000400	54111010	85×2^{-10}	1.764×2^{-9}
2	04010000	01000000	2^{-1}	
3	1C000400	04010000	2^{-2}	
4	00000000	00000000	2^{-1}	
5	1C000400	04010000	2^{-2}	
6	04010000	01000000	2^{-1}	
7	1D000400	54111010	85×2^{-10}	
C	1D000400	50101010		

4 Discussion

4.1 Attack Strategy

Since the approximate probability of a linear expression for 6-round is larger than that for 7-round and $N = c \times p'^{-2}$ holds, the 2-Round Elimination strategy is better than 1-Round Elimination from the standpoint of the required number of pairs for attack. However, 2-Round Elimination is infeasible, since the number of effective text bits, t, and the number of effective key bits, k, satisfy $t, k = 24 \sim 30$ roughly, and the processing amount is $O(2^{42\sim48})$ in 2-Round Elimination where we assume $N = 2^{18}$, since Biham's linear expression for 6-round satisfies $p' = 2^{-9}$, where the Biham's iterative 4-round expression [B94] is applied to 6-round.

Let us estimate t and k for Biham's 7-round linear expression, and those for our expression for 7-round, assuming the 1-Round Elimination Technique. The processing amount of an attack using our linear expression is $O(2^{36\sim40})$, since $t, k = 20 \sim 24$ holds roughly and $p' = 1.149 \times 2^{-8}$. The processing amount of an attack of 1-Round Elimination using Biham's 7-round expression is $O(2^{24\sim30})$ using **Algorithm 1**, since $t, k = 12 \sim 15$ and $p' = 2^{-11}$. The number of counters, U_i and T_j, required by **Algorithm 1** is $2^{12\sim15}$, which is acceptable.

We decided to adopt the **1-Round Elimination Technique** that requires us to analyze the following equation:

$$\begin{aligned} P_L[16,23,25,26,31] \oplus C_H[31] \oplus C_L[16,23,25,26] \\ \oplus F_8(C_H \oplus C_L, K_8)[23,25,31] = S. \end{aligned} \tag{3}$$

Our linear expression is effective for the later phases of an attack to derive subkeys other than those derived from the above equation.

4.2 Comparison with DES

The best expression can be obtained by an exhaustive search algorithm against DES [M93, M94]. Since the number of active S-Boxes, which are approximated with a certain masking value, at the first and last rounds of F-function is 2 and the bit length of data input to each S-Box is 6, the number of effective key bits is 12 in Equation (2).

On the other hand, since the byte rotation is built in implicitly between S-Boxes, the number of effective key bits and effective text bits seems to be $24 \sim 30$, which is larger than is true with DES. Thus 2-Round Elimination is infeasible in FEAL, which it is efficient in DES. Unfortunately, since we don't have any practical search algorithm to obtain the best expression of FEAL, there might be a better linear expression than Biham's.

How about the effective key and text bits? The closer from the right side an input bit is to a bit position related to a reference point output by the eighth F-function, the more strongly the value of the input bit determines the value of the XOR operation performed on the reference points, $F_8(C_H \oplus C_L, K_8)[23,25,31]$ in Equation (3). Therefore, the *effective key bits* should be subdivided into *explored key bits* and *detected key bits* for an attack against FEAL. Note that since each key bit input to an S-Box of DES influences all output bits more equally than that of FEAL, detected key bits are identical to explored key bits in DES. As a result, the treatment of effective key bits is simpler in an attack against DES than against FEAL. The similar discussion is valid in the treatment of effective text bits, which provides the number of counters, U_i. Thus there are various strategies to reduce the number of effective (explored/detected) key/text bits in an attack against FEAL.

Concerning the parameter, N, of FEAL–N, where N means the iteration number of F-function, it seems that while FEAL–32 is as secure as DES against Differential Cryptanalysis, FEAL–16 is as secure as DES from the standpoint of Linear Cryptanalysis, since the number of key bits which are explored by the attack is 12 with the 14-round linear expression with probability of 1.192×2^{-21} in DES, while it is $12 \sim 15$ with the 15-round linear expression with probability of 2^{-23} in FEAL assuming the Biham's iterative 4-round expression is applied to the 15-round case.

5 Experimentation Results

The following information was described in [OA94]:

(1) A table relating the success rate, the number of pairs of plaintexts and ciphertexts, and the effective key bits needed to solve Equation (3),
(2) How to derive the remaining values of all subkeys, and
(3) How to improve the success rate.

6 Concluding Remarks

It has been confirmed that the entire subkeys used in FEAL–8 can be derived from 2^{25} known plaintexts with a success rate approximately 70% spending about 1 hour, from 2^{26} known plaintexts with a success rate about 100% spending a little over 1 hour using a WS (SPARCstation 10 Model 30).

It seems that while FEAL–32 is as secure as the 16-round DES against Differential Cryptanalysis, FEAL–16 is as secure as it from the standpoint of Linear Cryptanalysis if we restrict ourselves to Matsui's implementation technique using Biham's linear expression.

There are several open problems:

(1) Search algorithm to obtain the best expression of FEAL,
(2) More efficient technique than **Algorithm 1**, and
(3) More efficient strategy for reducing the numbers of effective text bits and effective key bits in an attack against FEAL–8.

References

[B94] E. Biham, "On Matsui's Linear Cryptanalysis," EUROCRYPT'94

[CG91] A. Tardy-Corfdir and H. Gilbert, "A known plaintext attack of FEAL–4 and FEAL–6," CRYPTO'91

[M93] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," EUROCRYPT'93

[M94] M. Matsui, "On Correlation between the Order of S-Boxes and the strength of DES," EUROCRYPT'94

[MY92] M. Matsui and A. Yamagishi, "A New Method for Known Plaintext Attack of FEAL Cipher," EUROCRYPT'92

[MSS88] S. Miyaguchi, A. Shiraishi and A. Shimizu, "Fast Data Encipherment algorithm FEAL–8," Review of Electrical Communication Laboratories, Vol. 36, No. 4, 1988

[OA94] K.Ohta and K.Aoki, "Linear Cryptanalysis of the Fast Data Encipherment Algorithm," Technical Report of IEICE Japan, ISEC94-5, May, 1994 (which contains more information than this paper.)