Best Differential Characteristic Search of FEAL

Kazumaro Aoki[1], Kunio Kobayashi[2*], and Shiho Moriai[3**]

[1] NTT Laboratories
[2] School of Science and Engineering, Waseda University
[3] Information & Communication Security Project,
Telecommunications Advancement Organization of Japan

Abstract. This paper presents the results of the best differential characteristic search of FEAL.

The search algorithm for the best differential characteristic (best linear expression) was already presented by Matsui, and improvements on this algorithm were presented by Moriai et al. We further improve the speed of the search algorithm. For example, the search time for the 7-round best differential characteristic of FEAL is reduced to about 10 minutes (Pentium/166 MHz), which is about $2^{12.6}$ times faster than Matsui's algorithm. Moreover, we determine all the best differential characteristics of FEAL for up to 32 rounds assuming all S-boxes are independent.

As a result, we confirm that the N-round ($7 \leq N \leq 32$) best differential characteristic probability of FEAL is 2^{-2N}, which was found by Biham. For N = 6, we find 6-round differential characteristics with a greater probability, 2^{-11}, than that previously discovered, 2^{-12}.

1 Introduction

Since the introduction of differential cryptanalysis [BS91], evaluating the security of symmetric block ciphers against differential cryptanalysis has become an important research topic. Roughly speaking, we can evaluate the security of differential cryptanalysis using the best differential characteristic probability. The search algorithm for the best differential characteristic (best linear expression) of DES-like cryptosystems was already presented by Matsui [M95], and improvements on this algorithm were presented by Moriai et al. [MAO96]. However, if we apply these algorithms to the search for the best differential characteristic of FEAL [SM88, MKOM90], we cannot complete a search in a practical amount of time due to the enormous number of search candidates.

This paper proposes improvements on the algorithms introduced in [M95, MAO96] and presents the results of applying this improved algorithm to the search for the best differential characteristic of FEAL[4]. For example, the search for the 7-round best differential characteristic of FEAL requires about 10 minutes (Pentium/166MHz), which is about $2^{12\ 6}$ times faster than Matsui's algorithm.

[*] Part of this research was done during his 1995 summer intern at NTT Laboratories.
[**] This research was done at NTT Laboratories.
[4] The best linear expression of FEAL is obtained in [MAO96].

As a result, we confirm that the N-round ($7 \leq N \leq 32$) best differential characteristic probability of FEAL is 2^{-2N}, which was already known.

Strictly speaking, the security of Markov ciphers[5] against differential cryptanalysis would be better evaluated by the maximum average of the differential probability[6] than the best differential characteristic probability [LMM91]. However, it is very difficult to determine the maximum average of the differential probability of a block cipher and to evaluate the upper bound of the maximum average of the differential probability in a practical range. Therefore, at present,

- the security of block ciphers against differential cryptanalysis is evaluated by the best differential characteristic probability, or
- some block ciphers are designed in a manner that facilitates evaluating the maximum average of differential probability.

Requiring a large amount of time is not particularly problematic when applying the search algorithm for the best differential characteristic to an existing cipher. However, *designers* must repeatedly apply it to draft ciphers in the design process, for example, in order to select better S-boxes. Thus, it is indispensable that the time complexity of the search algorithm be reduced. It is important for the fast search algorithm to determine the *best* differential characteristic (linear expression). For example, [LSK95] proposed a fast search algorithm that finds *effective* linear expressions, but they are not particular about the optimality of the linear probability. Our search algorithm can determine the best differential characteristic probability faster than ever.

2 Notation

$\mathrm{BEST_N}$: N-round best differential characteristic probability
$\mathrm{CAND_N}$: temporal value of $\mathrm{BEST_N}$
ΔX_r: r-th round input difference
ΔY_r: r-th round output difference
$p_r = p_r(\Delta X_r, \Delta Y_r)$: r-th round differential characteristic probability
$\oplus$: bit-wise *exclusive or* operation
$S_d(x, y)$: S-box of FEAL; $x + y + d \bmod 2^8$

We define operator "$\oplus$" as having a higher priority than operator "$+$," and operator "$+$" as having a higher priority than operator "mod."

3 Previous Results

3.1 Biham's Result

Biham found several differential characteristics of FEAL. The best differential characteristic probabilities of FEAL he showed are listed in Table 1 [BS93].

[5] FEAL is a Markov cipher.

[6] Note that the maximum average of the differential probability is greater than the best differential characteristic probability.

Round (N)	Differential characteristic probability
$N \le 3$	1
$N = 4$	2^{-3}
$N = 5$	2^{-4}
$N \ge 6$	2^{-2N}

Table 1. Biham's results

3.2 Matsui's Algorithm

Matsui proposed a search algorithm for DES-like cryptosystems that determines $\mathrm{BEST_N}$ ($N \ge 3$) and the corresponding differential characteristics using the knowledge of BEST_r ($r < N$) [M95].

Algorithm 1 (Matsui's Algorithm).

Preparation: *Determine the initial value of* $\mathrm{CAND_N}$, *so that* $\mathrm{CAND_N}$ *will be as large as possible but smaller than the best differential characteristic probability.*

1-st round search: *For each candidate for* ΔX_1, *do the following:*
- *Choose* ΔY_1 *which maximizes* p_1.
- *Go to the 2-nd round search if* $p_1 \ge \dfrac{\mathrm{CAND_N}}{\mathrm{BEST_{N-1}}}$ *holds.*

2-nd round search: *For each candidate for* ΔX_2 *and* ΔY_2, *do the following:*
- *Go to the 3-rd round search if* $p_1 p_2 \ge \dfrac{\mathrm{CAND_N}}{\mathrm{BEST_{N-2}}}$ *holds.*

r-th round search ($3 \le r \le N - 1$): *Let* $\Delta X_r = \Delta Y_{r-1} \oplus \Delta X_{r-2}$ *and for each candidate for* ΔY_r, *do the following:*
- *Go to the* $(r+1)$*-th round search if* $\prod_{i=1}^{r} p_i \ge \dfrac{\mathrm{CAND_N}}{\mathrm{BEST}_{N-r}}$ *holds.*

N-th round search:
- *Let* $\Delta X_N = \Delta Y_{N-1} \oplus \Delta X_{N-2}$.
- *Choose* ΔY_N *which maximizes* p_N.
- *Let* $\mathrm{CAND_N} = \prod_{i=1}^{N} p_i$ *if* $\prod_{i=1}^{N} p_i \ge \mathrm{CAND_N}$ *holds.*

As a result, we have $\mathrm{BEST_N} = \mathrm{CAND_N}$.

3.3 Improved Algorithm (Moriai et al.)

Moriai et al. introduced the concept of *search patterns*. These patterns reduce the search complexity by detecting the unnecessary search candidates before the search. This method works because detection process requires only the probability of differential characteristics for each round and no differential characteristics.

A search pattern used in the search for the N-round best differential characteristic is a set of N probabilities, and each probability is a differential characteristic probability for each round. Their algorithm examines whether differential characteristics with probability $\mathrm{CAND_N}$ ($\mathrm{N} \geq 3$) exist and finds the differential characteristics, if any, using the knowledge of BEST_r ($r < \mathrm{N}$) [MAO96]. Their algorithm is shown below.

Algorithm 2 (Moriai et al. Algorithm).

1. *Generate all the search patterns* $(q_1, q_2, \ldots, q_\mathrm{N})$ *according to the conditions for Algorithm 1 which concern only the differential characteristics probabilities.*
2. *Discard the search patterns which satisfy the following conditions.*

$$\exists i, r \ (1 \leq i \leq \mathrm{N}, i + r - 1 < \mathrm{N}); \prod_{j=i}^{i+r-1} q_j > \mathrm{BEST}_r$$

3. *Discard either search pattern* $(q_1, q_2, \ldots, q_\mathrm{N})$ *or* $(q_\mathrm{N}, q_{\mathrm{N}-1}, \ldots, q_1)$ *whichever has more search candidates.*
4. *Search the differential characteristics corresponding to search pattern* $(q_1, q_2, \ldots, q_\mathrm{N})$ *using Algorithm 1 with all the inequalities replaced by equalities.*

4 Proposed Algorithms

Algorithm 2 discards only the unnecessary search patterns that satisfy the two conditions described above. However, we can discard more search patterns without loss of search exhaustivity. In sections 4.1 and 4.2 we present our improved algorithms and apply them to FEAL[7]. They are useful especially when the differential characteristic probability is of the powers of 2, for example, those for addition and (almost) bent functions, but they are applicable to other DES-like cryptosystems. Section 4.3 describes the generalization of our algorithm, particularly how to treat search patterns.

4.1 Using Presearch Based on Algorithm 2

Algorithm 2 introduces the search patterns to consider the probability of each round, but does not use the pattern itself. Taking this into consideration, we improve the search algorithm for the best differential characteristics.

Consider the search for 5-round differential characteristics of FEAL for example. In this case, we know all the 4-round search patterns corresponding to differential characteristics with probability 2^{-3} shown below when we complete a search for the 4-round differential characteristics.

$$(2^{-1}, 1, 2^{-1}, 2^{-1}), \ (2^{-1}, 2^{-1}, 1, 2^{-1}) \tag{1}$$

[7] Here we assume that all S-boxes are independent.

On the other hand, all search patterns of the 5-round with probability 2^{-3} which should be searched for by Algorithm 2 are as follows:

$$(1,1,1,2^{-3},1),\ (1,1,2^{-1},2^{-2},1),\ (1,1,2^{-2},2^{-1},1)\ ,$$
$$(1,1,2^{-3},1,1),\ (1,2^{-1},1,2^{-2},1),\ \text{and}\ (1,2^{-1},2^{-1},2^{-1},1)\ .$$

All these search patterns have interior 4-round search patterns with probability 2^{-3}. However, none of the 4-round search patterns (1) matches them. Thus the differential characteristics corresponding to these search patterns do not exist, and we do not have to search these search patterns. We also know that there is no 5-round differential characteristic with probability 2^{-3} without conducting a search.

Next, consider 5-round differential characteristics with probability 2^{-4}. In this case, search patterns for which Algorithm 2 searches are as follows.

1:$(1,1,1,2^{-3},2^{-1})$ **2**:$(1,1,1,2^{-4},1)$ **3**:$(1,1,2^{-1},2^{-2},2^{-1})$
4:$(1,1,2^{-1},2^{-3},1)$ **5**:$(1,1,2^{-2},2^{-1},2^{-1})$ **6**:$(1,1,2^{-2},2^{-2},1)$
7:$(1,1,2^{-3},1,2^{-1})$ **8**:$(1,1,2^{-3},2^{-1},1)$ **9**:$(1,1,2^{-4},1,1)$
10:$(1,2^{-1},1,2^{-2},2^{-1})$ **11**:$(1,2^{-1},1,2^{-3},1)$ **12**:$(1,2^{-1},2^{-1},2^{-1},2^{-1})$
13:$(1,2^{-1},2^{-1},2^{-2},1)$ **14**:$(1,2^{-1},2^{-2},1,2^{-1})$ **15**:$(1,2^{-1},2^{-2},2^{-1},1)$
16:$(1,2^{-2},1,2^{-1},2^{-1})$ **17**:$(1,2^{-2},1,2^{-2},1)$ **18**:$(2^{-1},1,1,2^{-2},2^{-1})$
19:$(2^{-1},1,1,2^{-3},1)$ **20**:$(2^{-1},1,2^{-1},2^{-1},2^{-1})$ **21**:$(2^{-1},1,2^{-1},2^{-2},1)$
22:$(2^{-1},1,2^{-2},1,2^{-1})$ **23**:$(2^{-1},2^{-1},1,2^{-1},2^{-1})$

Note that the search patterns are numbered **1** to **23**. Search patterns numbered **1**, **3**, **5**, **7**, **10**, **12**, **14**, **16**, **18**, **20**, **22**, and **23** have probability 2^{-3} from the 1-st round to 4-th round. Considering the results of the search for the 4-round differential characteristic (1), we have only to search search patterns **20** and **23**. Moreover, search patterns **19**, **20**, **21**, and **23** have probability 2^{-3} from the 2-nd round to 5-th round. Similarly, as a result of the 4-round differential characteristic search (1), only search pattern **23** survives. From the discussion above, the number of search patterns which should be searched decreases from 23 to 10. The remaining search patterns are **2**, **4**, **6**, **8**, **9**, **11**, **13**, **15**, **17**, and **23**.

Furthermore, the information which is used for discarding search patterns need not be that of the best differential characteristic. Not only the search patterns of the best differential characteristic, but also those of the differential characteristics with lower probabilities are useful. We know that no 3-round differential characteristic with probability 2^{-1} exists as the result of the search, for example. If we use this condition, search patterns **4** and **11** need not be searched.

We summarize this algorithm as follows.

Algorithm 3.

1. *Search r-round* ($r <$ N) *differential characteristics with various probabilities, and compile information to the extent possible whether or not the search patterns exist for each round and probability.* (*presearch phase*)

2. *In Algorithm 2, discard the search patterns which do not exist using the information from the presearch phase.*

The information from the presearch phase is also useful in performing a presearch. Moreover, presearches can be completed faster since the presearch may be stopped for a search pattern as soon as the first differential characteristic of the search pattern is determined.

4.2 Using Presearch Based on Algorithm 1

This section proposes further improvements on the search algorithm. Search patterns are useful tools for discarding unnecessary search candidates. However, Algorithm 2 repeats the search process for each search pattern, and sometimes repeats similar computations. The search algorithm described in this section can reduce the complexity based on the following.

1. Improving the right side of the inequalities in Algorithm 1.
2. Combining the same computation repeated several times into one.

In the previous section, we found that the number of search patterns which Algorithm 3 should search is 8, when we searched for the 5-round differential characteristics with a probability of 2^{-4} using presearch information obtained from 3-round differential characteristics with a probability of 2^{-1} and 4-round differential characteristics with a probability of 2^{-3}.

Of course, the correct results can be obtained if we search all eight search patterns mentioned above. However, some search patterns have the same probability in the 1-st and 2-nd rounds. For example, search patterns **2**, **6**, **8**, and **9** have the same search pattern from the 1-st round to the 2-nd round $(1,1)$. This means that the same computation for the search is done repeatedly for the 1-st and the 2-nd rounds which dominates the search complexity.

In Algorithm 1, the inequality shown below determines whether or not the search for more than r-rounds is needed.

$$\prod_{i=1}^{r} p_i \geq \frac{\mathrm{CAND_N}}{\mathrm{BEST_{N-}}_r} \tag{2}$$

Since the right side of (2) is constant, it can be determined before Algorithm 1 starts. The greater the right side of (2) is, the smaller the search complexity is. We want the right side of (2) to be as large as possible while still maintaining search exhaustivity.

We define the set comprising the right sides of (2) for r $(1 \leq r \leq \mathrm{N})$ as $(R_1^{(j)}, R_2^{(j)}, \ldots, R_{\mathrm{N}}^{(j)})$[8]. From the definition of $R_r^{(j)}$, the maximum $R_r^{(j)}$ $(1 \leq r \leq \mathrm{N})$ for which Algorithm 1 searches the differential characteristics with a search pattern $(q_1^{(j)}, q_2^{(j)}, \ldots, q_{\mathrm{N}}^{(j)})$ is;

$$R_r^{(j)} = \prod_{i=1}^{r} q_i^{(j)} \ . \tag{3}$$

[8] We also define $\mathrm{BEST_0} = 1$.

Thus, differential characteristics with all search patterns $(q_1^{(j)}, q_2^{(j)}, \ldots, q_{\mathrm{N}}^{(j)})$ will be searched if we set

$$R_r = \min_j R_r^{(j)}$$

where $(R_1^{(j)}, R_2^{(j)}, \ldots, R_{\mathrm{N}}^{(j)})$ is calculated using (3).

The following algorithm was derived from the discussion above.

Algorithm 4.

1. *Derive search patterns* $(q_1^{(j)}, q_2^{(j)}, \ldots, q_{\mathrm{N}}^{(j)})$ *using Algorithm 3.*
2. *For each search pattern, calculate* $(R_1^{(j)}, R_2^{(j)}, \ldots, R_{\mathrm{N}}^{(j)})$ *where* $R_r^{(j)} = \prod_{i=1}^{r} q_i^{(j)}$ $(1 \leq r \leq \mathrm{N})$.
3. *Let* $R_r = \min_j R_r^{(j)}$.
4. *Run Algorithm 1 with the right side of inequalities* $\frac{\mathrm{CAND_N}}{\mathrm{BEST_{N-r}}}$ *replaced by* R_r $(1 \leq r \leq \mathrm{N})$.

Some search patterns which Algorithm 3 should search may have considerably smaller probabilities from the 1-st and 2-nd rounds than the others. In this case, some search patterns should be searched directly, and Algorithm 4 is applied to other search patterns.

4.3 Generalization of Algorithm 3

In this section we generalize Algorithm 3 so that we can apply it to other DES-like cryptosystems whose differential characteristic probability also takes variables other than the power of 2. In Algorithm 5, the variable $\mathrm{TENT_N}$ is used for treating search patterns effectively.

Algorithm 5 (when p_r is not a power of 2).

1. *Let* $\mathrm{TENT_N} = 2^{\lfloor \log_2 \mathrm{BEST_{N-1}} \rfloor + \mathrm{N}}$ *and* $\mathrm{CAND_N} = \mathrm{BEST_{N-1}}$.
2. *Generate all the search patterns* $(q_1, q_2, \ldots, q_{\mathrm{N}})$ *so that* q_r $(1 \leq r \leq N)$ *should be powers of* 2*, and* $2 \times \mathrm{TENT_N} \geq \prod_{r=1}^{\mathrm{N}} q_r \geq \mathrm{TENT_N}$ *should hold in the similar way as Algorithm 2.*
3. *Discard the search patterns similarly as Algorithm 3.*
4. *Perform Algorithm 1 such that at the r-th round search* $(1 \leq r \leq \mathrm{N})$ *the differential characteristics whose r-round differential characteristic probability* p_r *satisfies the following conditions:*

$$q_r \geq p_r > 2^{\log_2 q_r - 1} \quad \text{and} \quad \prod_{i=1}^{r} p_i \geq \mathrm{CAND_N} .$$

5. *If* $\mathrm{TENT_N} \geq 2^{\lceil \log_2 \mathrm{CAND_N} \rceil}$ *holds, and* $\mathrm{CAND_N}$ *is revised even once, i.e. a differential characteristic probability that is better than all previous is found, let* $\mathrm{TENT_N} = 2^{-1} \times \mathrm{TENT_N}$ *and go to the 2-nd step.*

   Otherwise, we have $\mathrm{BEST_N} = \mathrm{CAND_N}$.

Though in the algorithm above we use the power of 2 as q_r and $\mathrm{TENT_N}$, appropriate numbers, for example 4, may be used.

5 Small Techniques

All algorithms presented above require differential characteristics of the F-function. It is impractical to calculate differential characteristic of the F-function for FEAL every time it is required because a long time is required. It is also impractical to calculate and store all differential characteristics of the F-function in advance because of time and space requirements.

We regard all S_d functions to be independent[9]. We adopt this method: calculate the differential characteristics of the S_d function in advance, and calculate differential characteristics of the F-function every time it is required with a very low level of complexity.

However, this method still requires a long time and an enormous amount of memory. We decrease the complexity using the following properties of the S_d function [S96].

Note that constants and variables in the following theorems and conjectures are l-bit strings.

Theorem 1 (Equivalence of S_0 and S_1). *For any* (a, b, c), *equations*

$$\begin{aligned} x \oplus a + y \oplus b \bmod 2^l &= (x + y) \oplus c \bmod 2^l \quad \textit{and} \\ x \oplus a + y \oplus b + 1 \bmod 2^l &= (x + y + 1) \oplus c \bmod 2^l \end{aligned}$$

hold with the same probability.

Theorem 2 (Distribution of differential probability of addition). *For any* (a, b, c), *probability with which*

$$x \oplus a + y \oplus b \bmod 2^l = (x + y) \oplus c \bmod 2^l$$

holds is 0 or a power of 2.

[9] The best differential characteristic (linear expression) searches previously reported in References [M95, MAO96, TSM95] were based on the same assumption.

Sketch of proof of Theorems 1 and 2: First, prove the propositions of Theorems 1 and 2 in linear cryptanalysis by studying the carry propagation of addition. Second, translate the results to those in differential cryptanalysis using the Walsh transformation [CV95].

Conjecture 1. *If*

$$a \oplus b = a' \oplus b' \quad \textit{and}$$
$$a + b \equiv a' + b' \pmod{2^l}$$

holds, equations

$$x \oplus a + y \oplus b \bmod 2^l = (x + y) \oplus c \bmod 2^l \quad \textit{and}$$
$$x \oplus a' + y \oplus b' \bmod 2^l = (x + y) \oplus c \bmod 2^l$$

hold with the same probability.

In case of $l = 8$, a computer exhaustive search proves that this conjecture is correct.

By using Conjecture 1, the data (a, b, c) and (a', b', c') can be made up into the datum $(a \oplus b, a + b \bmod 2^l, c)$ to reduce the amount of required memory.

Conjecture 2 (# of non-0 entries in diff. char. dist. table). *The number of pairs (a, b, c) which satisfy equation*

$$x \oplus a + y \oplus b \bmod 2^l = (x + y) \oplus c \bmod 2^l \quad \textit{with non-0 probability}$$

is $4 \cdot 7^{l-1}$.

In the case of $l \leq 8$, a computer exhaustive search proves that this conjecture is correct.

Conjecture 3. *The number of pairs $(a \oplus b, a + b \bmod 2^l, c)$ which satisfies equation*

$$x \oplus a + y \oplus b \bmod 2^l = (x + y) \oplus c \bmod 2^l \quad \textit{with non-0 probability}$$

is $2 \cdot 5^{l-1}$, which is, surprisingly, the same as the number of non-zero entries in the linear distribution table.

In the case of $l = 8$, a computer exhaustive search proves that this conjecture is correct.

6 Search Experiments and Results

The complexity of Algorithm 1 can be estimated using the number of search candidates for the 1-st and 2-nd rounds [MAO96]. Figure 1 illustrates the number of search candidates for the 1-st and 2-nd rounds of FEAL using Algorithms 1 and 4 where we set CAND_N to the best differential characteristic probability. Note that we ignore the presearch complexity in the case of Algorithm 4. We perform a presearch based on Table 2. A 7-round search for FEAL requires the most search time, about 10 minutes (Pentium/166 MHz) using Algorithm 4.

Figure 2 illustrates the best differential characteristic probability of FEAL.

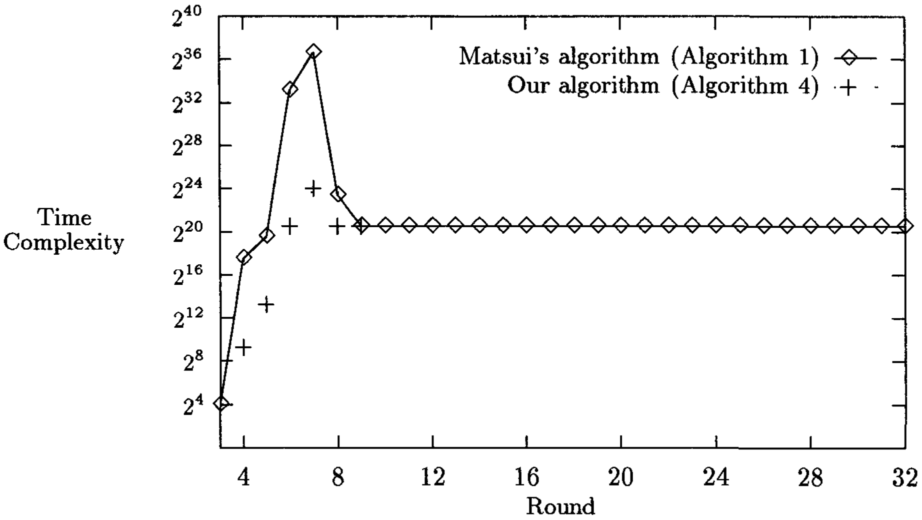

Fig. 1. Complexity of the search for the best differential characteristic probability of FEAL

7 Conclusion

We succeeded in completing the search for the best differential characteristics of FEAL for up to 32 rounds by improving the known search algorithm. We found 6-round differential characteristics with a greater probability, 2^{-11} than that previously discovered, 2^{-12}. All the best 6-round characteristics are illustrated in Fig. 3. We also confirmed that the N-round ($7 \leq \mathrm{N} \leq 32$) best differential characteristic probability is $2^{-2\mathrm{N}}$. These best differential characteristics were previously determined but it was not confirmed whether or not these differential characteristics were the best [BS93]. We conclude that FEAL–32 is secure against differential cryptanalysis in that the best differential characteristic probability is sufficiently small.

Due to the duality of differential cryptanalysis and linear cryptanalysis [M95], we can apply the idea of Algorithms 3, 4, and 5 to the search for the best linear expression.

The remaining problem is to develop an algorithm whose complexity is minimal taking into consideration the presearch complexity in Algorithms 3, 4, and 5.

References

[BS91] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1, pp. 3–72, 1991. (The extended abstract was presented at CRYPTO'90).

Number of rounds N	Presearch information	
for search	Number of rounds	Probability
4	3	$2^{-0}, 2^{-1}, 2^{-2}$
5	3	$2^{-0}, 2^{-1}, 2^{-2}, 2^{-3}$
	4	2^{-3}
6	3	$2^{-0}, 2^{-1}, 2^{-2}, 2^{-3}, 2^{-4}$
	4	$2^{-3}, 2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}, 2^{-9}$
	5	$2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}, 2^{-9}$
7	3	$2^{-0}, 2^{-1}, 2^{-2}, 2^{-3}, 2^{-4}$
	4	$2^{-3}, 2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}, 2^{-9}$
	5	$2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}, 2^{-9}$
	6	2^{-11}
8	3	$2^{-0}, 2^{-1}, 2^{-2}, 2^{-3}, 2^{-4}$
	4	$2^{-3}, 2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}, 2^{-9}$
	5	$2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}, 2^{-9}$
	6	2^{-11}
	7	2^{-14}
9	3	$2^{-0}, 2^{-1}, 2^{-2}, 2^{-3}, 2^{-4}$
	4	$2^{-3}, 2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}, 2^{-9}$
	5	$2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}, 2^{-9}$
	6	2^{-11}
	7	2^{-14}
	8	2^{-16}

Table 2. Used presearch information

r	ΔY_r	ΔX_r	p_r	r	ΔY_r	ΔX_r	p_{r_1}	r	ΔY_r	ΔX_r	p_{r_1}
1	02000000	80800000	1	1	00000008	00000202	2^{-1}	1	00000202	00800282	2^{-1}
2	80800000	A0008000	2^{-2}	2	00000202	00800282	2^{-1}	2	00800282	80A0A2A2	2^{-3}
3	00000000	00000000	1	3	00000000	00000000	1	3	00000000	00000000	1
4	80800000	A0008000	2^{-2}	4	00000202	00800282	2^{-1}	4	00800282	80A0A2A2	2^{-3}
5	02000000	80800000	1	5	00000008	00000202	2^{-1}	5	00000202	00800282	2^{-1}
6	A8882080	A2008000	2^{-7}	6	8020A2A0	0080028A	2^{-7}	6	0080028A	80A0A0A0	2^{-3}

(The differential characteristics which are the differential characteristics above turned upside down are also the best 6-round differential characteristics.)

Table 3. Best 6-round differential characteristics

[BS93] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard.* Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[CV95] F. Chabaud and S. Vaudenay. Links Between Differential and Linear Cryptanalysis. In A. D. Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, Volume 950 of *Lecture Notes in Computer Science*, pp. 356–365. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[LMM91] X. Lai, J. L. Massey, and S. Murphy. Markov Ciphers and Differential Cryptanalysis. In D. W. Davies, editor, *Advances in Cryptology — EURO-*

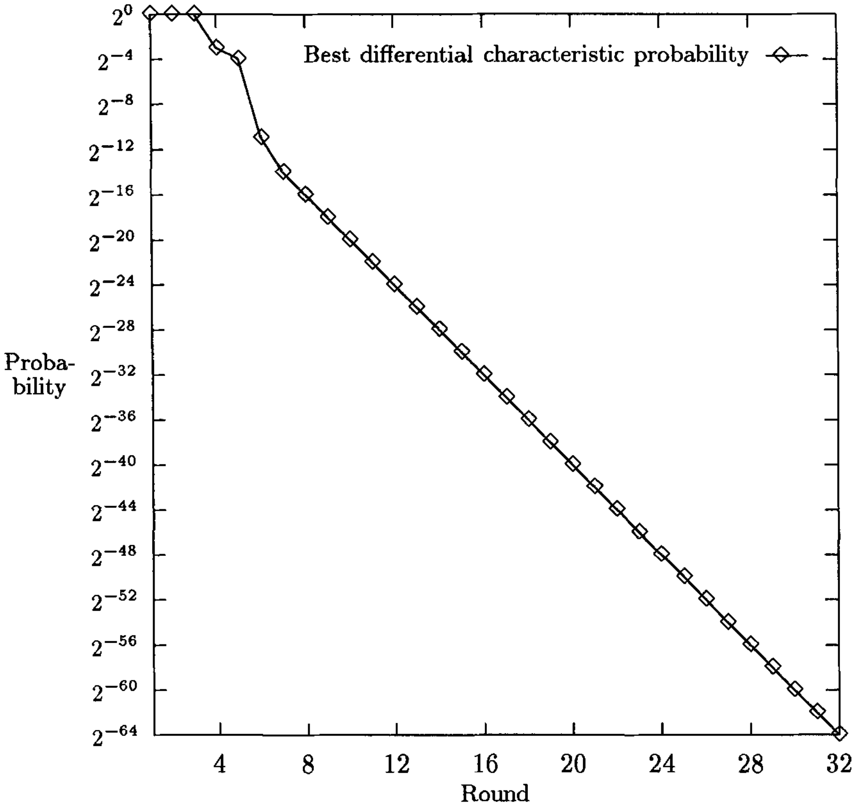

Fig. 2. Best differential characteristic probability of FEAL

CRYPT'91, Volume 547 of *Lecture Notes in Computer Science*, pp. 17–38. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[LSK95] S. Lee, S. H. Sung, and K. Kim. An Efficient Method to Find the Linear Expressions for Linear Cryptanalysis. In *1995 Japan-Korea Joint Workshop on Information Security and Cryptology*, pp. 183–190, Inuyama, Aichi, JAPAN, 1995. ISEC Group of IEICE (Japan) and KIISC (Korea).

[M95] M. Matsui. On Correlation Between the Order of S-boxes and the Strength of DES. In A. D. Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, Volume 950 of *Lecture Notes in Computer Science*, pp. 366–375. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[MAO96] S. Moriai, K. Aoki, and K. Ohta. The Best Linear Expression Search of FEAL. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, Vol. E79-A, No. 1, pp. 2–11, 1996. (The extended abstract was presented at CRYPTO'95).

[MKOM90] S. Miyaguchi, S. Kurihara, K. Ohta, and H. Morita. Expansion of FEAL Cipher. *Review of Electrical Communication Laboratories*, Vol. 2, No. 6, pp. 117–127, 1990.

[S96] M. Sugita. Private communications, 1996.

[SM88] A. Shimizu and S. Miyaguchi. Fast Data Encipherment Algorithm FEAL. In *Advances in Cryptology — EUROCRYPT'87*, Volume 304 of *Lecture Notes in Computer Science*, pp. 267–278. Springer-Verlag, Berlin, Heidelberg, New York, 1988.

[TSM95] T. Tokita, T. Sorimachi, and M. Matsui. Linear Cryptanalysis of LOKI and s^2-DES. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology — ASIACRYPT'94*, Volume 917 of *Lecture Notes in Computer Science*, pp. 293–303. Springer-Verlag, Berlin, Heidelberg, New York, 1995.