International Symposium on Information Theory and its Applications, ISITA2008
Auckland, New Zealand, 7-10, December, 2008

Cryptanalysis of CLEFIA Using Multiple Impossible Differentials

Yukiyasu TSUNOO†, Etsuko TSUJIHARA‡, Maki SHIGERI††,
Tomoyasu SUZAKI†, and Takeshi KAWABATA††

† NEC Corporation,
1753, Shimonumabe, Nakahara-Ku, Kawasaki,
Kanagawa 211-8666, Japan
E-mail: {tsunoo@bl, t-suzaki@cb}.jp.nec.com

‡ Y.D.K.Co.,Ltd.,
1288 Oshitate, Inagi,
Tokyo 206-0811, Japan
E-mail: etsuko-t@ghn.ydkinc.co.jp

†† NEC Software Hokuriku, Ltd.,
1, Anyouji, Hakusan,
Ishikawa 920-2141, Japan
E-mail: {m-shigeri, t-kawabata}@pb.jp.nec.com

Abstract

This paper reports impossible differential cryptanalysis on the 128-bit block cipher CLEFIA that was proposed in 2007. It is known that there are the 9-round impossible differentials in CLEFIA. This paper presents the several results of impossible differential attacks using multiple impossible differentials. For key lengths of 128, 192 and 256 bits, it is possible to apply impossible differential attacks to 12-round, 13-round and 14-round CLEFIA. For the case of a 128-bit key, this attack is the most efficient compared with previous results. For key lengths of 192 and 256 bits, the numbers of chosen plaintexts are the least.

1. INTRODUCTION

Differential attacks [1] and linear attacks [2] are quite well known attack methods applied to block ciphers. Guaranteeing security against differential attacks and linear attacks is an important problem in the design of block ciphers. One known method of evaluating security against such attacks uses the minimum number of active S-boxes. Shirai et al. proposed in 2004 the diffusion switching mechanism (DSM), a method of designing a Feistel structure block cipher that can guarantee a large minimum number of active S-boxes [3, 4]. In 2007, CLEFIA, a 128-bit block cipher designed using DSM, was proposed [5]. The designers of CLEFIA adopted a four-branch generalized Feistel structure to achieve both a small implementation size and high speed. The generalized Feistel structure tends to require more rounds to guarantee security than does an ordinary Feistel structure, but CLEFIA can guarantee resistance to differential attacks and linear attacks with a small number of rounds because of the use of DSM.

The impossible differential attack [6] is a method, that was first applied against Skipjack, to reject wrong key candidates by using input difference and output difference pairs whose probabilities are zero (impossible differentials). The attack often uses the impossible differentials that are dependent on the structure of the data processing part of a target cipher. Impossible differential attack is a considerable threat especially for the generalized Feistel structure. Since CLEFIA is a generalized Feistel structure, the impossible differential attack is an effective attack against CLEFIA. In [7, 8, 9], it was shown that there are previously unknown 9-round impossible differentials in CLEFIA. Furthermore, [7, 8, 9] reported the results of impossible differential attacks using those impossible differentials. [7, 8, 9] showed that 12-round, 13-round and 14-round CLEFIA can be broken for key lengths of 128, 192 and 256 bits[1].

This paper reports the several results of impossible differential attacks using multiple impossible differentials. For the case of a 128-bit key, it is possible to apply the impossible differential attack to 12-round CLEFIA. The number of chosen plaintexts is $2^{108.0}$ and the time complexity is 2^{108}. This result is the most efficient compared with previous results. For key lengths of 192 and 256 bits, the numbers of chosen plaintexts are the least.

We describe the CLEFIA structure shortly in Sect. 2, show the 9-round impossible differentials in Sect.

[1] In [8], the time complexities of the key recovery attack on 14-round and 15-round CLEFIA are not accurate. The 15-round CLEFIA can not be broken.

Table 1: Differential values for α_{in} and α_{out}

Type	$w_b(\alpha_{in})$, $w_b(\alpha_{out})$	α_{in}	α_{out}
A	1, 1	$[0_{(8)}, 0_{(8)}, 0_{(8)}, X_{(8)}]$ $[0_{(8)}, 0_{(8)}, X_{(8)}, 0_{(8)}]$ $[0_{(8)}, X_{(8)}, 0_{(8)}, 0_{(8)}]$ $[X_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$	$[0_{(8)}, 0_{(8)}, Y_{(8)}, 0_{(8)}]$, $[0_{(8)}, Y_{(8)}, 0_{(8)}, 0_{(8)}]$, $[Y_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$ $[0_{(8)}, 0_{(8)}, 0_{(8)}, Y_{(8)}]$, $[0_{(8)}, Y_{(8)}, 0_{(8)}, 0_{(8)}]$, $[Y_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$ $[0_{(8)}, 0_{(8)}, 0_{(8)}, Y_{(8)}]$, $[0_{(8)}, 0_{(8)}, Y_{(8)}, 0_{(8)}]$, $[Y_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$ $[0_{(8)}, 0_{(8)}, 0_{(8)}, Y_{(8)}]$, $[0_{(8)}, 0_{(8)}, Y_{(8)}, 0_{(8)}]$, $[0_{(8)}, Y_{(8)}, 0_{(8)}, 0_{(8)}]$
B	1, 2	$[0_{(8)}, 0_{(8)}, 0_{(8)}, X_{(8)}]$ $[0_{(8)}, 0_{(8)}, X_{(8)}, 0_{(8)}]$ $[0_{(8)}, X_{(8)}, 0_{(8)}, 0_{(8)}]$ $[X_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$	$[0_{(8)}, 0_{(8)}, Y_{(8)}, Z_{(8)}]$, $[0_{(8)}, Y_{(8)}, 0_{(8)}, Z_{(8)}]$, $[Y_{(8)}, 0_{(8)}, 0_{(8)}, Z_{(8)}]$ $[0_{(8)}, 0_{(8)}, Y_{(8)}, Z_{(8)}]$, $[0_{(8)}, Y_{(8)}, Z_{(8)}, 0_{(8)}]$, $[Y_{(8)}, 0_{(8)}, Z_{(8)}, 0_{(8)}]$ $[0_{(8)}, Y_{(8)}, 0_{(8)}, Z_{(8)}]$, $[0_{(8)}, Y_{(8)}, Z_{(8)}, 0_{(8)}]$, $[Y_{(8)}, Z_{(8)}, 0_{(8)}, 0_{(8)}]$ $[Y_{(8)}, 0_{(8)}, 0_{(8)}, Z_{(8)}]$, $[Y_{(8)}, 0_{(8)}, Z_{(8)}, 0_{(8)}]$, $[Y_{(8)}, Z_{(8)}, 0_{(8)}, 0_{(8)}]$
C	2, 1	$[0_{(8)}, 0_{(8)}, Y_{(8)}, Z_{(8)}]$ $[0_{(8)}, Y_{(8)}, 0_{(8)}, Z_{(8)}]$ $[Y_{(8)}, 0_{(8)}, 0_{(8)}, Z_{(8)}]$ $[0_{(8)}, Y_{(8)}, Z_{(8)}, 0_{(8)}]$ $[Y_{(8)}, 0_{(8)}, Z_{(8)}, 0_{(8)}]$ $[Y_{(8)}, Z_{(8)}, 0_{(8)}, 0_{(8)}]$	$[0_{(8)}, 0_{(8)}, 0_{(8)}, X_{(8)}]$, $[0_{(8)}, 0_{(8)}, X_{(8)}, 0_{(8)}]$ $[0_{(8)}, 0_{(8)}, 0_{(8)}, X_{(8)}]$, $[0_{(8)}, X_{(8)}, 0_{(8)}, 0_{(8)}]$ $[0_{(8)}, 0_{(8)}, 0_{(8)}, X_{(8)}]$, $[X_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$ $[0_{(8)}, 0_{(8)}, X_{(8)}, 0_{(8)}]$, $[0_{(8)}, X_{(8)}, 0_{(8)}, 0_{(8)}]$ $[0_{(8)}, 0_{(8)}, X_{(8)}, 0_{(8)}]$, $[X_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$ $[0_{(8)}, X_{(8)}, 0_{(8)}, 0_{(8)}]$, $[X_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$

3, present the several results of impossible differential attacks using multiple impossible differentials in Sect. 4. Section 5 concludes this paper.

2. DESCRIPTION OF CLEFIA

2.1. Notation

We use the following notation in this paper.

$a_{(b)}$	b is the bit length of a If the bit length of a is known, (b) is omitted.
$a \mid b$	The concatenation of a and b
$[a, b]$	The vector representation of $a \mid b$
$[x^{\{i,0\}}, x^{\{i,1\}}, x^{\{i,2\}}, x^{\{i,3\}}]$	i-round output data, $x^{\{i,j\}} \in \{0,1\}^{32}$ The plaintext is $[x^{\{0,0\}}, x^{\{0,1\}}, x^{\{0,2\}}, x^{\{0,3\}}]$.
$[C^{\{i,0\}}, C^{\{i,1\}}, C^{\{i,2\}}, C^{\{i,3\}}]$	The i-round CLEFIA ciphertext
$a \oplus b$	Bit-wise exclusive OR of a and b (addition over GF(2^n))
Δa	Difference for a (difference over GF(2^n))
$w_b(a)$	For an $8n$-bit string $a = a_{0(8)} \mid a_{1(8)} \mid \ldots \mid a_{n-1(8)}$, $w_b(a)$ denotes the number of non-zero a_is.

2.2. Structure of Data Processing Part

CLEFIA is a block cipher that has a block length of 128 bits and key lengths of 128, 192, and 256 bits. The data processing part is a four-branch generalized Feistel structure with two parallel F functions (F_0, F_1) per round. The numbers of respective rounds for 128-bit, 192-bit and 256-bit keys are 18, 22 and 26. The full description of the CLEFIA algorithm is described in [5].

3. NINE-ROUND IMPOSSIBLE DIFFERENTIALS

It is known that there are the following two 9-round impossible differentials in CLEFIA [7, 8, 9].

$$[0, 0, 0, \alpha_{in(32)}] \not\rightarrow {}_{9r}[0, 0, 0, \alpha_{out(32)}]$$
$$[0, \alpha_{in(32)}, 0, 0] \not\rightarrow {}_{9r}[0, \alpha_{out(32)}, 0, 0]$$

The α_{in} and α_{out} are the differences shown in Table 1. The $X_{(8)}$, $Y_{(8)}$ and $Z_{(8)}$ are arbitrary non-zero values.

4. IMPOSSIBLE DIFFERENTIAL ATTACKS ON REDUCED-ROUND CLEFIA

In this section, we explain the impossible differential attacks using the 9-round impossible differential $[0, 0, 0, \alpha_{in}] \not\rightarrow {}_{9r}[0, 0, 0, \alpha_{out}]$.

The impossible differentials used for the attacks are as follows.

Case 1) One impossible differential
  Case 1-1) One pair of (α_{in},α_{out}) in type B
  Case 1-2) One pair of (α_{in},α_{out}) in type C
Case 2) Multiple impossible differentials
  Case 2-1) All of the 12 pairs of (α_{in},α_{out}) in type A
  Case 2-2) All of the 12 pairs of (α_{in},α_{out}) in type B
  Case 2-3) All of the 12 pairs of (α_{in},α_{out}) in type C

Table 2: Results of impossible differential attacks

Reference	Number of rounds	Key length	Key recovery (bits)	Chosen plaintexts	Time complexity (encryptions)	Amount of memory (blocks)
[7]	12	128,192,256	80	$2^{118.9}$	2^{119}	2^{73}
This paper (Case 1), [9]	12	128,192,256	88	$2^{111.0}$	2^{111}	2^{81}
This paper (Case 2-1)	12	128,192,256	128	$2^{116.0}$	2^{116}	2^{99}
This paper (Case 2-2)	12	128,192,256	128	$2^{108.0}$	2^{108}	2^{99}
This paper (Case 2-3)	12	128,192,256	128	$2^{108.0}$	2^{108}	2^{108}
[7]	13	192,256	144	$2^{119.8}$	2^{146}	2^{120}
This paper (Case 1), [9]	13	192,256	152	$2^{111.8}$	2^{155}	2^{112}
This paper (Case 2-1)	13	192,256	192	$2^{116.6}$	2^{171}	2^{97}
This paper (Case 2-2)	13	192,256	192	$2^{108.6}$	2^{179}	2^{109}
This paper (Case 2-3)	13	192,256	192	$2^{108.6}$	2^{171}	2^{105}
[7]	14	256	208	$2^{120.3}$	2^{212}	2^{121}
This paper (Case 1), [9]	14	256	216	$2^{112.3}$	2^{220}	2^{113}
This paper (Case 2-1)	14	256	256	$2^{117.0}$	2^{236}	2^{117}
This paper (Case 2-2)	14	256	256	$2^{109.0}$	2^{244}	2^{109}
This paper (Case 2-3)	14	256	256	$2^{109.0}$	2^{236}	2^{109}

4.1. Results of Impossible Differential Attacks

The results of the impossible differential attacks on reduced-round CLEFIA are presented in Table 2. In an attack using case 1-1 and an attack using case 1-2, the same number of key bits can be recovered with the same number of chosen plaintexts and the same time complexity ("This paper (Case 1), [9]" in Table 2). In attacks using case 2 with a key length of 128 bits, key recovery attacks with the least number of chosen plaintexts and the least time complexity on 12-round CLEFIA are possible for case 2-2 or case 2-3 ("This paper (Case 2-2) and (Case 2-3)" in Table 2). In attacks using case 2, key recovery attack with the least number of chosen plaintexts and the least time complexity is possible on 13-round CLEFIA with a key length of 192 bits and on 14-round CLEFIA with a key length of 256 bits for case 2-3 ("This paper (Case 2-3)" in Table 2).

We consider the reason to be that fewer chosen plaintexts are required when 12 pairs of impossible differentials (α_{in}, α_{out}) are used at the same time than when only one pair is used. Because the non-zero byte positions of the 12 (α_{in}, α_{out}) pairs are different, the number of key bits that must be assumed increases and the number of chosen ciphertext pairs required for the attacks also increases. However, 12 times as many chosen ciphertext pairs can be obtained from one set of 2^{64} chosen plaintexts with the third and fourth words fixed, then the number of chosen plaintexts required for the attacks decreases by a factor of about 2^3. The reasons that 12 times as many chosen ciphertext pairs can be obtained from one chosen plaintext set are listed below.

- Multiple α_{in} have different non-zero byte positions, so more plaintext pairs can be made than when only one α_{in} is used.
- Multiple α_{out} have different non-zero byte positions, so more chosen ciphertext pairs can be obtained than when only one α_{out} is used.

In the following subsections, we explain key recovery attacks on 12-round CLEFIA with case 2-2 and key recovery attacks on 13-round and 14-round CLEFIA with case 2-3. The attacks described in this paper use less than 2^{128} blocks of memory, which is the same as in [7] and [9].

4.2. Key Recovery Attack on 12-round CLEFIA

In this section, we explain a key recovery attack on 12-round CLEFIA with case 2-2.

Movement of WK_0 and WK_2

Move WK_0 and place it at the bit-wise exclusive OR with the first-round output $x^{\{1,0\}}$. Move WK_2 and place it at the bit-wise exclusive OR with the tenth-round output $x^{\{10,2\}}$ and the bit-wise exclusive OR with RK_{21} (Figure 1). These movements are equivalent transformations.

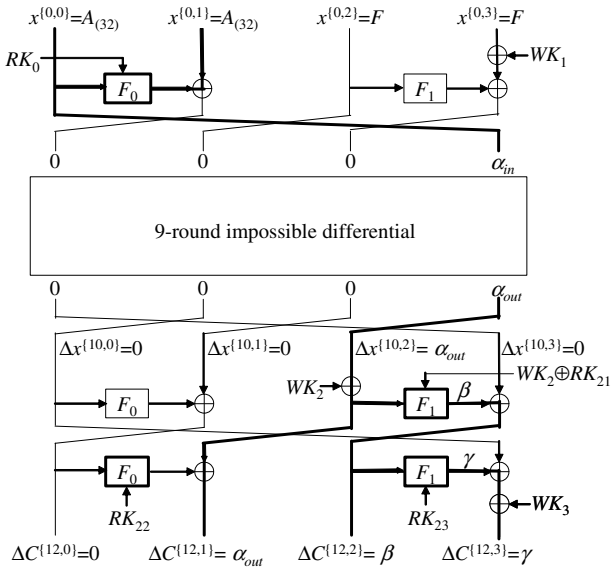

Figure 1: Impossible Differential Attack on 12-round CLEFIA

Key Recovery

The RK_0, $WK_2 \oplus RK_{21}$, RK_{22}, and RK_{23} keys can be recovered, for a total of 128 bits.

The procedure for the key recovery attack on 12-round CLEFIA is described below.

Preparation: Let $RK_0 = [RK_{0,0(8)}, RK_{0,1(8)}, RK_{0,2(8)}, RK_{0,3(8)}]$. Set up key tables for storing whether the value of $(WK_2 \oplus RK_{21})|RK_{22}|RK_{23}$ is correct or wrong. The key tables accord with the cases when from $RK_{0,0}$ to $RK_{0,3}$ respectively take values from 0 to 255. Denote these tables as $SvKey[i][j][k]$; $i \in \{0, 1, 2, 3\}$, $j \in \{0, 1, ..., 255\}$, $k \in \{0, ..., 2^{96} - 1\}$ and initialize all of the entries of $SvKey$ to 0 (meaning "correct"). The amount of memory is $2^{96} \cdot 2^8 \cdot 4 = 2^{106}$ bits $= 2^{99}$ blocks.

1. Encrypt a 2^{64} chosen plaintext set $[A_{(32)}, A_{(32)}, F_{(32)}, F_{(32)}]$ that has the third and fourth words fixed to obtain the ciphertexts. Here, $A_{(32)}|A_{(32)}$ are all of the values 0,1, ..., $2^{64}-1$ and F is an arbitrary constant.
for(i = 0, 1, 2, 3) {
for(j = 0, 1, ..., 255) {

Assume $RK_{0,i} = j$, and choose sets of 2^8 ciphertexts for which the first three words of the second round input are fixed and the fourth word $x^{\{1,3\}}$ of the second round input are as described below.[2]

If $i = 0$, then $x^{\{1,3\}} = [A_{(8)}, F_{(8)}, F_{(8)}, F_{(8)}]$.
If $i = 1$, then $x^{\{1,3\}} = [F_{(8)}, A_{(8)}, F_{(8)}, F_{(8)}]$.
If $i = 2$, then $x^{\{1,3\}} = [F_{(8)}, F_{(8)}, A_{(8)}, F_{(8)}]$.
If $i = 3$, then $x^{\{1,3\}} = [F_{(8)}, F_{(8)}, F_{(8)}, A_{(8)}]$.

This set of 2^8 ciphertexts is referred to as the structure. From a set of 2^{64} chosen plaintexts, $2^{32} \cdot 2^{24}$ structures can be obtained. For each structure, choose the ciphertext pairs whose differences are $[0, \alpha_{out}, \beta_{(32)}, \gamma_{(32)}]$; $\beta \in \{M_1(\alpha_{out^*})\}$, $\gamma \in \{1, 2, ..., 2^{32} - 1\}$, where α_{out^*} is α_{out} with all the non-zero byte positions set to any integer value from 1 to 255. For example, if α_{out} is $[0, 0, Y, Z]$, then α_{out^*} can be any of the 255^2 values of $[0, 0, 1, 1]$, $[0, 0, 1, 2]$, ..., $[0, 0, 255, 255]$. The probability of these ciphertext pairs existing is $2^{-32-16-16+0} \cdot 3 = 2^{-64} \cdot 3$.

For the chosen ciphertext pairs, compute k', the values of $(WK_2 \oplus RK_{21})|RK_{22}|RK_{23}$ for which the tenth-round output differences are $[0, 0, \alpha_{out}, 0]$. RK_{22} is guessed by an exhaustive search. Use the differential table[3] to find the values of $WK_2 \oplus RK_{21}$ and RK_{23}. Set $SvKey[i][j][k']$ to 1 (meaning "wrong").

The total number of keys that can be rejected by using one chosen ciphertext pair is $2^{16} \cdot 2^{32} \cdot 2^0 = 2^{48}$, so the key rejection rate is $2^{48}/2^{96} = 2^{-48}$.
} }

Repeat the above process $2^{44.0}$ times. The total number of chosen plaintexts is $2^{64} \cdot 2^{44.0} = 2^{108.0}$.

2. The $j_0|j_1|j_2|j_3|k''$ $(0 \le j_0, j_1, j_2, j_3 \le 255)$ such that all of $SvKey[0][j_0][k'']$, $SvKey[1][j_1][k'']$, $SvKey[2][j_2][k'']$, and $SvKey[3][j_3][k'']$ are zero is the correct value of $RK_0|(WK_2 \oplus RK_{21})|RK_{22}|RK_{23}$.

The number of chosen ciphertext pairs, N, required to narrow down the key candidates to the correct key is approximately $2^{54.5}$ from the following equation.

$$2^{128}(1 - 2^{-48})^N = 1$$

The number of chosen ciphertext pairs, N, that can be obtained from $2^{108.0}$ chosen plaintexts is about $2^{54.5}$ from the following equation.

$$N = 2^{44} \cdot 2^{32} \cdot 2^{24} \cdot_{2^8} C_2 \cdot 4 \cdot (2^{-64} \cdot 3) = 2^{54.5}$$

The time complexity is as follows.
(1) For obtaining the ciphertexts : $2^{108.0}$ encryptions
(2) For reducing the key candidates :
$2^8 \cdot 4 \cdot N/4 \cdot 2^{32} = 2^{94.5}$ F-function computations
$< 2^{90}$ encryptions
Accordingly, the time complexity is 2^{108} encryptions.

In the key recovery attack on 12-round CLEFIA, having $SvKey$ can reduce the time complexity from 2^{114} to 2^{108}. Without $SvKey$, the time complexity for

[2] Use the method described in Sect. 3.3 of [7].

[3] A table that records the input value pairs for which occur the input-output differences for each of the input differences and output differences of the S-boxes or F functions.

narrowing the keys down is as follows.

$2^{32} \cdot N \cdot 2^{32} = 2^{118.5}$ F-function computations

$< 2^{114}$ encryptions

4.3. Key Recovery Attack on 13-round CLEFIA

Here we describe the 13-round CLEFIA key recovery attack with case 2-3.

Movement of WK_0, WK_2 and WK_3

Move WK_0 and place it at the bit-wise exclusive OR with the first-round output $x^{\{1,0\}}$. Move WK_2 and place it at the bit-wise exclusive OR with the 11th-round output $x^{\{11,2\}}$ and the bit-wise exclusive OR with RK_{23}. Move WK_3 and place it at the bit-wise exclusive OR with the 11th-round output $x^{\{11,0\}}$ and the bit-wise exclusive OR with RK_{22}.

Key Recovery

The RK_0, RK_{21}, $WK_3 \oplus RK_{22}$, $WK_2 \oplus RK_{23}$, RK_{24}, and RK_{25} keys can be recovered for a total of 192 bits.

The procedure for the key recovery attack on 13-round CLEFIA is described below.

Preparation: Set up tables to store the ciphertext pairs whose differences are [α_{out}, $\beta'_{(32)}$, γ, $\delta_{(32)}$]. The tables used in this attack accord with the case in which the respective values of $RK_{0,i}|RK_{0,j}$ ($i \neq j$, $0 \leq i, j \leq 5$) are from 0 to $2^{16} - 1$. Here, $\beta' \in \{M_0(\alpha_{out^*}) \oplus M_1(\alpha_{out^{**}})\}$, $\gamma \in \{1, 2, ..., 2^{32} - 1\}$, and $\delta \in \{1, 2, ..., 2^{32} - 1\}$. The α_{out^*} and $\alpha_{out^{**}}$ respectively are α_{out} with all the non-zero byte positions set to any integer value from 1 to 255. Denote the table for storing the ciphertext pairs as $SvCtext[i][j][k]$; $i \in \{0, 1, 2, ..., 5\}$, $j \in \{0, 1, ..., 2^{16} - 1\}$, $k \in \{0, 1, ..., 2^{87.1}/6 - 1\}$. To simplify the explanation, we omit k in the following. If i is any of 0, 1, ..., 5, then the respective two bytes of RK_0 are $RK_{0,0}$ and $RK_{0,1}$, $RK_{0,0}$ and $RK_{0,2}, ..., RK_{0,2}$ and $RK_{0,3}$. The amount of memory is $2 \cdot 2^{87.1}/6 \cdot 2^{16} \cdot 6 \approx 2^{105}$ blocks.

1. Encrypt a 2^{64} chosen plaintext set [A, A, F, F] that has the third and fourth words fixed to obtain the ciphertexts.
for(i = 0, 1, ..., 5) {
for(j = 0, 1, ..., $2^{16} - 1$) {

Assume that the two-byte value of RK_0 selected by i is j and choose sets of 2^{16} ciphertexts for which words 1, 2 and 3 of the second round input are fixed and the fourth word $x^{\{1,3\}}$ of the second round input are as follows.

If $i = 0$, then $x^{\{1,3\}} = [A_{(8)}, A_{(8)}, F_{(8)}, F_{(8)}]$.

If $i = 1$, then $x^{\{1,3\}} = [A_{(8)}, F_{(8)}, A_{(8)}, F_{(8)}]$.

:

If $i = 5$, then $x^{\{1,3\}} = [F_{(8)}, F_{(8)}, A_{(8)}, A_{(8)}]$.

This set of 2^{16} ciphertexts is called the structure. From a set of 2^{64} chosen plaintexts, $2^{32} \cdot 2^{16}$ structures can be obtained. For each structure, choose the ciphertext pairs for whose differences are [α_{out}, β', γ, δ] and store them in $SvCtext[i][j]$. The probability of these ciphertext pairs existing is $2^{-24-16+0+0} \cdot 2 = 2^{-40} \cdot 2$.
} }

Repeat the above process $2^{44.6}$ times. The total number of chosen plaintexts is $2^{64} \cdot 2^{44.6} = 2^{108.6}$.

2. Prepare a key table to narrow down $RK_{21}|(WK_2 \oplus RK_{23})|RK_{25}$ and denote the table as $Key[k]; k \in \{0, ..., 2^{96} - 1\}$.
for($j_0|j_1|j_2|j_3$ = 0, 1, ..., $2^{32} - 1$) {
for(j_4 = 0, 1, ..., $2^{64} - 1$;
j_4 is the value of $(WK_3 \oplus RK_{22})|RK_{24}$) {
Initialize all Key entries to 0.
For $SvCtext[0][j_0|j_1]$, $SvCtext[1][j_0|j_2]$, ..., $SvCtext[5][j_2|j_3]$, compute the values of $RK_{21}|(WK_2 \oplus RK_{23})|RK_{25}$, k', for which the 10th-round output differences are [0, 0, α_{out}, 0]. The values of RK_{21} and $WK_2 \oplus RK_{23}$ and RK_{25} are obtained by using the differential table. Set $Key[k']$ to 1.

The total number of keys that can be rejected with one pair of $SvCtext$ is $2^{24} \cdot 2^0 \cdot 2^0 = 2^{24}$, so the key rejection rate is $2^{24}/2^{96} = 2^{-72}$. Because the input difference of the 13th-round F_0 function is α_{out} and the input difference of M_0 of the 13th-round F_0 function can be uniquely determined from β' [4], one byte of RK_{24} can be determined for each $SvCtext$ pair. Only in the case that this value and the one byte of RK_{24} of j_4 are the same can the $SvCtext$ be used to narrow down the keys. The number of $SvCtext$ pair that can be used is decreased by a factor of 2^8, so the number of chosen ciphertext pairs required for attack, N, increases by a factor of 2^8.

If 0 remains in the Key entry and $Key[k''] = 0$, $j_0|j_1|j_2|j_3|j_4|k''$ is the correct value of $RK_0|(WK_3 \oplus RK_{22})|RK_{24}|RK_{21}|(WK_2 \oplus RK_{23})|RK_{25}$.
} }

The number of chosen ciphertext pairs, N, required to narrow down the key candidates to the correct key is approximately $2^{87.1}$ from the following equation.

$$2^{192}(1 - 2^{-72})^{N'} = 1, \quad N = 2^8 \cdot N' = 2^{87.1}$$

The number of chosen ciphertext pairs, N, that can be obtained from $2^{108.6}$ chosen plaintexts is about $2^{87.1}$

[4] From proposition 3 of [8], the 11th-round M_1 input difference and the 13th-round M_0 input difference can be uniquely determined from the ciphertext difference β'.

from the following equation.

$$N = 2^{44.6} \cdot 2^{32} \cdot 2^{16} \cdot_{2^{16}} C_2 \cdot 6 \cdot (2^{-40} \cdot 2) = 2^{87.1}$$

The time complexity is as follows.
(1) For obtaining the ciphertexts : $2^{108.6}$ encryptions
(2) For reducing the key candidates :
$2^{32} \cdot N/2^8 \cdot 2^{64} = 2^{175.1}$ F-function computations
$< 2^{171}$ encryptions
Accordingly, the time complexity is 2^{171} encryptions.

4.4. Key Recovery Attack on 14-round CLEFIA

We explain the key recovery attack on 14-round CLEFIA with case 2-3. The RK_0, $WK_3 \oplus RK_{21}$, RK_{22}, RK_{23}, $WK_3 \oplus RK_{24}$, $WK_2 \oplus RK_{25}$, RK_{26}, and RK_{27} keys can be recovered, for a total of 256 bits.

Adding an exhaustive search for the 14th-round keys RK_{26} and RK_{27} to the key recovery attack on 13-round CLEFIA allows an attack on the 14-round CLEFIA.

The number of chosen plaintexts is $2^{109.0}$ from the following.

The number of chosen ciphertext pairs, N, required to narrow down the key candidates to the correct key is approximately $2^{111.5}$ from the following equation.

$$2^{256}(1 - 2^{-72})^{N'} = 1, \quad N = 2^8 \cdot 2^{24} \cdot N' = 2^{111.5}$$

The number of chosen ciphertext pairs, N, that can be obtained from $2^{109.0}$ chosen plaintexts is about $2^{87.1}$ from the following equation.

$$N = 2^{45.0} \cdot 2^{32} \cdot 2^{16} \cdot_{2^{16}} C_2 \cdot 6 \cdot (2^{-16} \cdot 2) = 2^{111.5}$$

The time complexity is as follows.
(1) For obtaining the ciphertexts : $2^{109.0}$ encryptions
(2) For reducing the key candidates :
$2^{32} \cdot N/(2^8 \cdot 2^{24}) \cdot 2^{128} \cdot 2 = 2^{240.5}$ F-function computations $< 2^{236}$ encryptions
Accordingly, the time complexity is 2^{236} encryptions.

5. CONCLUSION

It is known that there are the 9-round impossible differentials in CLEFIA. In this paper, we have reported the several results of impossible differential attacks using multiple impossible differentials.

Though these impossible differential attacks can recover the number of more key bits than results of [7, 8, 9], we have been able to reduce the number of chosen plaintexts. For key lengths of 128 bits, we have been able to reduce both the number of chosen plaintexts and the time complexity using multiple impossible differentials. This result is the most efficient compared with previous results. For key lengths of 192 and 256 bits, the numbers of chosen plaintexts are the least. The impossible differential attacks presented in this paper do not directly affect the security of the full-round CLEFIA, because the numbers of CLEFIA rounds are 18 for a key length of 128 bits, 22 for a 192-bit key and 26 for a 256-bit key.

References

[1] E. Biham, and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," CRYPTO'90, LNCS 537, pp. 2–21, Springer-Verlag, 1990.

[2] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," EUROCRYPT'93, LNCS 765, pp. 386–397, Springer-Verlag, 1994.

[3] T. Shirai, and B. Preneel, "On Feistel Ciphers Using Optimal Diffusion Mappings Across Multiple Rounds," ASIACRYPT 2004, LNCS 3329, pp. 1–15, Springer-Verlag, 2004.

[4] T. Shirai, and K. Shibutani, "On Feistel Structures Using a Diffusion Switching Mechanism," FSE 2006, LNCS 4047, pp. 41–56, Springer-Verlag, 2006.

[5] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit Blockcipher CLEFIA," FSE 2007, LNCS 4593, pp. 181–195, Springer-Verlag, 2007.

[6] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials," EUROCRYPT'99, LNCS 1592, pp. 12–23, Springer-Verlag, 1999.

[7] Y. Tsunoo, E. Tsujihara, M. Shigeri, T. Saito, T. Suzaki, and H. Kubo, "Impossible Differential Cryptanalysis of CLEFIA," FSE 2008, LNCS 5086, pp. 398–411, Springer-Verlag, 2008.

[8] B. Sun, R. Li, M. Wang, P. Li, and C. Li, "Impossible Differential Cryptanalysis of CLEFIA," ePrint 2008/151.
Available at http://eprint.iacr.org/2008/151.

[9] E. Tsujihara, M. Shigeri, T. Suzaki, T. Kawabata, and Y. Tsunoo, "New Impossible Differentials of CLEFIA," Technical report of IEICE. ISEC, May 2008 (in Japanese).