Impossible Differential Cryptanalysis of CLEFIA

Yukiyasu Tsunoo[1], Etsuko Tsujihara[2], Maki Shigeri[3], Teruo Saito[3], Tomoyasu Suzaki[1], and Hiroyasu Kubo[3]

[1] NEC Corporation, 1753, Shimonumabe, Nakahara, Kawasaki 211-8666, Japan
{tsunoo@BL,t-suzaki@cb}.jp.nec.com
[2] Y.D.K.Co.,Ltd., 1288, Oshitate, Inagi-Shi, Tokyo 206-0811, Japan
etsuko-t@ghn.ydkinc.co.jp
[3] NEC Software Hokuriku, Ltd., 1,Anyoji, Hakusan, Ishikawa 920-2141, Japan
{m-shigeri@pb,t-saito@qh,h-kubo@ps}.jp.nec.com

Abstract. This paper reports impossible differential cryptanalysis on the 128-bit block cipher CLEFIA that was proposed in 2007, including new 9-round impossible differentials for CLEFIA, and the result of an impossible differential attack using them. For the case of a 128-bit key, it is possible to apply the impossible differential attack to CLEFIA reduced to 12 rounds. The number of chosen plaintexts required is $2^{118.9}$ and the time complexity is 2^{119}. For key lengths of 192 bits and 256 bits, it is possible to apply impossible differential attacks to 13-round and 14-round CLEFIA. The respective numbers of chosen plaintexts required are $2^{119.8}$ and $2^{120.3}$ and the respective time complexities are 2^{146} and 2^{212}. These impossible differential attacks are the strongest method for attacking reduced-round CLEFIA.

Key words: block cipher, CLEFIA, diffusion switching mechanism, generalized Feistel structure, impossible differential cryptanalysis.

1 Introduction

Differential attacks [2] and linear attacks [3] are the most common methods of attack 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 [4, 5]. In 2007, CLEFIA, a 128-bit block cipher designed using DSM, was proposed [6]. 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 [1] 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). Impossible differentials that are dependent on the basic structure of the data processing part are often used, and this method is a particular threat to the generalized Feistel structure. Since CLEFIA is a generalized Feistel structure, the impossible differential attack is an effective attack against CLEFIA. According to the designers, an evaluation of CLEFIA with respect to an impossible differential attack [6, 7] shows that there are 9-round impossible differentials in CLEFIA, and for a 128-bit key, a 10-round impossible differential attack is possible. For key lengths of 192 bits and 256 bits, 11-round and 12-round impossible differential attacks are possible.

In this paper, we show that there are previously unknown 9-round impossible differentials in CLEFIA and report the result of impossible differential attacks using those impossible differentials. These impossible differentials exist in structures that are designed using DSM. In the impossible differential attacks on CLEFIA described in this paper, 12-round CLEFIA can be broken for a 128-bit key. For key lengths of 192 bits and 256 bits, impossible differential attacks are respectively possible for 13-round and 14-round CLEFIA.

There have been no reports on the cryptanalysis of CLEFIA other than the evaluation by the designers. Accordingly, the strong attack method for CLEFIA up to now is the differential attack and linear attack described in the designers' evaluation, which shows the possibility of 12-round, 13-round, and 14-round attack for the respective key lengths of 128 bits, 192 bits, and 256 bits. Nevertheless, these results are values for guaranteeing security with respect to differential attacks or linear attacks; the numbers of rounds for establishing actual differential attacks or linear attacks are probably smaller. Accordingly, the impossible differential attacks described in this paper are the result for the most number of rounds as an actual attack method on CLEFIA.

In this paper, we describe the CLEFIA structure in Sect. 2, explain the newly discovered impossible differentials and present attack procedures against CLEFIA using those differentials in Sect. 3. Section 4 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 $a \mid b$
${}^t a$	Transposition of vector a or matrix a
$[x^{\{i,0\}}, x^{\{i,1\}}, x^{\{i,2\}}, x^{\{i,3\}}]$	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 $\mathrm{GF}(2^n)$)
Δa	Difference for a (difference over $\mathrm{GF}(2^n)$)
$w_b(a)$	For an $8n$-bit string $a = a_{0(8)} \,|\, a_{1(8)} \,|\, \ldots \,|\, a_{n-1(8)}$, $w_b(a)$ denotes the number of non-zero a_is.
$B(P)$	Branch number for function P $B(P) = min_{a \neq 0}\{w_b(a) + w_b(P(a))\}$

2.2 Structure

In this section, we explain only the data processing part of CLEFIA.

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 number of respective rounds r for 128-bit, 192-bit and 256-bit keys are 18, 22 and 26. The encryption function ENC_r generates 128-bit ciphertext from 128-bit plaintext, $2r$ 32-bit round keys $(RK_{0(32)}, \ldots, RK_{2r-1(32)})$, and four 32-bit whitening keys $(WK_0, \ldots, WK_3)$. The structure of the encryption function ENC_r is shown in Fig. 1. ENC_r is defined as follows.

ENC_r:
Step 1. $T_0 \,|\, T_1 \,|\, T_2 \,|\, T_3 \leftarrow x^{\{0,0\}} \,|\, (x^{\{0,1\}} \oplus WK_0) \,|\, x^{\{0,2\}} \,|\, (x^{\{0,3\}} \oplus WK_1)$
Step 2. For i=0 to $r-1$ do the following:
Step 2.1. $T_1 \leftarrow T_1 \oplus F_0(RK_{2i}, T_0)$, $T_3 \leftarrow T_3 \oplus F_1(RK_{2i+1}, T_2)$
Step 2.2. $T_0 \,|\, T_1 \,|\, T_2 \,|\, T_3 \leftarrow T_1 \,|\, T_2 \,|\, T_3 \,|\, T_0$
Step 3. $C^{\{r,0\}} \,|\, C^{\{r,1\}} \,|\, C^{\{r,2\}} \,|\, C^{\{r,3\}} \leftarrow T_3 \,|\, (T_0 \oplus WK_2) \,|\, T_1 \,|\, (T_2 \oplus WK_3)$

The two F functions, F_0 and F_1, have 32-bit data x and 32-bit key RK as input; they output the 32-bit data y. F_0 is defined as follows.

F_0:
Step 1. $T \leftarrow RK \oplus x$
Step 2. Let $T = T_{0(8)} \,|\, T_{1(8)} \,|\, T_{2(8)} \,|\, T_{3(8)}$
$T_0 \leftarrow S_0(T_0)$, $T_1 \leftarrow S_1(T_1)$, $T_2 \leftarrow S_0(T_2)$, $T_3 \leftarrow S_1(T_3)$
Step 3. Let $y = y_{0(8)} \,|\, y_{1(8)} \,|\, y_{2(8)} \,|\, y_{3(8)}$
${}^t[y_0, y_1, y_2, y_3] = M_0 \, {}^t[T_0, T_1, T_2, T_3]$

F_1 is defined by replacing the terms in F_0 as follows: S_0 is replaced with S_1, S_1 with S_0, and M_0 with M_1. The structures of F_0 and F_1 are shown in Fig. 2.

S_0 and S_1 are non-linear 8-bit S-boxes.

The two matrices M_0 and M_1 are defined as

$$M_0 = \begin{pmatrix} \mathrm{0x01} & \mathrm{0x02} & \mathrm{0x04} & \mathrm{0x06} \\ \mathrm{0x02} & \mathrm{0x01} & \mathrm{0x06} & \mathrm{0x04} \\ \mathrm{0x04} & \mathrm{0x06} & \mathrm{0x01} & \mathrm{0x02} \\ \mathrm{0x06} & \mathrm{0x04} & \mathrm{0x02} & \mathrm{0x01} \end{pmatrix}, \; M_1 = \begin{pmatrix} \mathrm{0x01} & \mathrm{0x08} & \mathrm{0x02} & \mathrm{0x0}a \\ \mathrm{0x08} & \mathrm{0x01} & \mathrm{0x0}a & \mathrm{0x02} \\ \mathrm{0x02} & \mathrm{0x0}a & \mathrm{0x01} & \mathrm{0x08} \\ \mathrm{0x0}a & \mathrm{0x02} & \mathrm{0x08} & \mathrm{0x01} \end{pmatrix}.$$

The multiplications between these matrices and vectors are performed in $GF(2^8)$ defined by the primitive polynomial $z^8 + z^4 + z^3 + z^2 + 1$.

M_0 and M_1 satisfy

$$B(M_0) = B(M_1) = 5,\ B(M_0 \,|\, M_1) = B({}^tM_0^{-1} \,|\, {}^tM_1^{-1}) = 5.$$

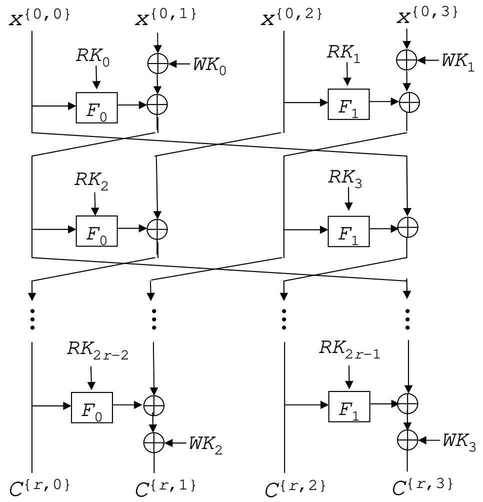

Fig. 1. Encryption function ENC_r

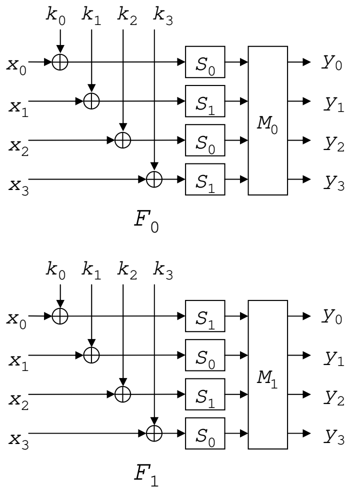

Fig. 2. Functions F_0 and F_1

3 Impossible Differential Attacks on CLEFIA

In this section, we present the new 9-round impossible differentials in Sect. 3.1, and explain the procedure for using those impossible differentials to attack CLEFIA in Sect. 3.2 and subsequent sections.

3.1 Nine-round impossible differentials of CLEFIA

The following two new 9-round impossible differentials are found in CLEFIA,

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

where α_{in} and α_{out} are the differences shown in Table 1. The $X_{(8)}$ and $Y_{(8)}$ in α_{in} and α_{out} are arbitrary non-zero values. These impossible differentials are entirely different from the impossible differentials found by the designers. The first impossible differential is represented in Fig. 3.

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

α_{in}	α_{out}
$[0_{(8)}, 0_{(8)}, 0_{(8)}, X_{(8)}]$	$[0_{(8)}, 0_{(8)}, Y_{(8)}, 0_{(8)}], [0_{(8)}, Y_{(8)}, 0_{(8)}, 0_{(8)}], [Y_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$
$[0_{(8)}, 0_{(8)}, X_{(8)}, 0_{(8)}]$	$[0_{(8)}, 0_{(8)}, 0_{(8)}, Y_{(8)}], [0_{(8)}, Y_{(8)}, 0_{(8)}, 0_{(8)}], [Y_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$
$[0_{(8)}, X_{(8)}, 0_{(8)}, 0_{(8)}]$	$[0_{(8)}, 0_{(8)}, 0_{(8)}, Y_{(8)}], [0_{(8)}, 0_{(8)}, Y_{(8)}, 0_{(8)}], [Y_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$
$[X_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$	$[0_{(8)}, 0_{(8)}, 0_{(8)}, Y_{(8)}], [0_{(8)}, 0_{(8)}, Y_{(8)}, 0_{(8)}], [0_{(8)}, Y_{(8)}, 0_{(8)}, 0_{(8)}]$

Here, we prove that where $\alpha_{in} = [0_{(8)}, 0_{(8)}, 0_{(8)}, X_{(8)}]$, and $\alpha_{out} = [Y_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]$, the probability of $[0_{(32)}, 0_{(32)}, 0_{(32)}, \alpha_{in}]$ occurring nine rounds after $[0_{(32)}, 0_{(32)}, 0_{(32)}, \alpha_{out}]$ is zero, which is to say that $[0, 0, 0, \alpha_{in}] \not\to_{9r} [0, 0, 0, \alpha_{out}]$ is an impossible differential. Other impossible differentials can be proven in the same way.

Proof. Assume that the input difference $\Delta x^{\{4,0\}}$ of the fifth-round F_0 function for when the input difference is $[0_{(32)}, 0_{(32)}, 0_{(32)}, [0_{(8)}, 0_{(8)}, 0_{(8)}, X_{(8)}]]$ and the input difference $\Delta x'^{\{4,0\}}$ of the fifth-round F_0 function for when the output difference is $[0_{(32)}, 0_{(32)}, 0_{(32)}, [Y_{(8)}, 0_{(8)}, 0_{(8)}, 0_{(8)}]]$ are the same.

$$\Delta x^{\{4,0\}} = \Delta x'^{\{4,0\}}. \tag{1}$$

The $\Delta x^{\{4,0\}}$ can be expressed using the fourth-round matrix M_0 and second-round matrix M_1 as

$$\begin{aligned} \Delta x^{\{4,0\}} &= M_0\, {}^t[0, 0, 0, X'] \oplus M_1\, {}^t[0, 0, 0, X''] \\ &= (M_0 \,|\, M_1)\, {}^t[0, 0, 0, X', 0, 0, 0, X''], \end{aligned} \tag{2}$$

where X' is the output difference for when the S_1 input difference is X, and X'' is the output difference for when the S_0 input difference is X; both are non-zero values.

Also, the $\Delta x'^{\{4,0\}}$ can be expressed using the 8th-round matrix M_0 and the 6th-round matrix M_1 as

$$\begin{aligned} \Delta x'^{\{4,0\}} &= M_0\, {}^t[Y', 0, 0, 0] \oplus M_1\, {}^t[Y'', 0, 0, 0] \\ &= (M_0 \,|\, M_1)\, {}^t[Y', 0, 0, 0, Y'', 0, 0, 0], \end{aligned} \tag{3}$$

where Y' is the output difference for when the S_0 input difference is Y and Y'' is the output difference for when the S_1 input difference is Y; both are non-zero values.

From (1), (2) and (3), we obtain

$$(M_0 \,|\, M_1)\, {}^t[Y', 0, 0, X', Y'', 0, 0, X''] = {}^t[0, 0, 0, 0] \tag{4}$$

because

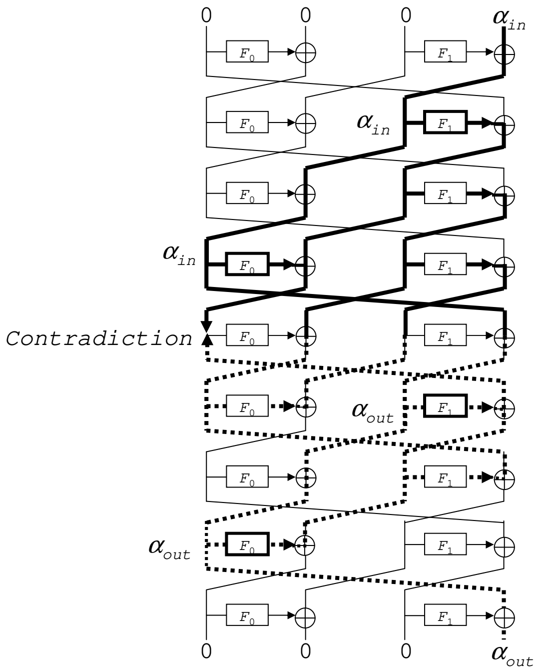

Fig. 3. Nine-round impossible differential

$$\begin{aligned}
&\Delta x^{\{4,0\}} \oplus \Delta' x^{\{4,0\}} \\
&= (M_0 \,|\, M_1)\,{}^t[0,0,0,X',0,0,0,X''] \oplus (M_0 \,|\, M_1)\,{}^t[Y',0,0,0,Y'',0,0,0] \\
&= (M_0 \,|\, M_1)\,{}^t([0,0,0,X',0,0,0,X''] \oplus [Y',0,0,0,Y'',0,0,0]) \\
&= (M_0 \,|\, M_1)\,{}^t[Y',0,0,X',Y'',0,0,X''].
\end{aligned}$$

From the CLEFIA specifications, the branch number of the concatenation matrix $M_0 \,|\, M_1$ is 5. Therefore

$$w_b([Y',0,0,X',Y'',0,0,X'']) + w_b((M_0 \,|\, M_1)\,{}^t[Y',0,0,X',Y'',0,0,X'']) \geq 5.$$

From $w_b([Y',0,0,X',Y'',0,0,X'']) = 4$, for the left side of (4),

$$w_b((M_0 \,|\, M_1)\,{}^t[Y',0,0,X',Y'',0,0,X'']) \geq 1. \tag{5}$$

Furthermore, for the right side of (4),

$$w_b([0,0,0,0]) = 0. \tag{6}$$

Equations (5) and (6) contradict (4).

Accordingly, $\Delta x^{\{4,0\}}$ and $\Delta x'^{\{4,0\}}$ cannot be equal and $[0,0,0,[0,0,0,X]] \not\to_{9r} [0,0,0,[Y,0,0,0]]$ is thus an impossible differential. $\square$

3.2 Key Recovery Attack on 11-round CLEFIA

In this section, we explain an impossible differential attack on 11-round CLEFIA using the 9-round impossible differentials presented in Sect. 3.1 as preparation for an impossible differential attack on 12-round CLEFIA which we show in Sect. 3.3. For simplicity of explanation in the next section, we regard the first-round output to be plaintext and present the attack procedure for the 11 rounds from the second round to the 12th round. Of the 9-round impossible differentials shown in Sect. 3.1, we describe the case for the input difference of $[0, 0, 0, [0, 0, 0, X]]$ and the output difference of $[0, 0, 0, [Y, 0, 0, 0]]$ as shown in Fig. 4. It is possible to recover RK_{22}, RK_{23}, and the most significant byte of $WK_2 \oplus RK_{21}$, which we represent as $RK'_{21,0(8)}$.

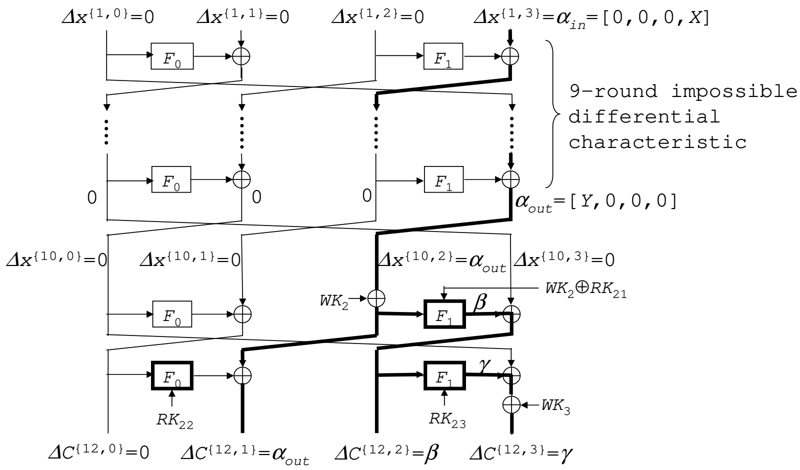

Fig. 4. Impossible differential attack on 11-round CLEFIA

Movement of Whitening key $\boldsymbol{WK_2}$. Move the whitening key WK_2, and place it at the bit-wise exclusive OR with the 10th-round output $x^{\{10,2\}}$ and bit-wise exclusive OR with RK_{21}. This movement is an equivalent transformation.

Key Recovery. Of the ciphertext pairs that correspond to the plaintext pairs for which the difference is $[0, 0, 0, [0, 0, 0, X]]$, choose those for which the ciphertext difference is $[0, [Y, 0, 0, 0], \beta_{(32)}, \gamma_{(32)}]$. Here, β represents the 255 values that can be obtained as the output difference when the input difference for M_1 is $[Y, 0, 0, 0]$; γ is a non-zero value. The probability of obtaining such ciphertext pairs is $1/2^{32} \cdot 255/2^{32} \cdot 255/2^{32} \cdot (2^{32} - 1)/2^{32} \approx 2^{-80}$.

For the chosen ciphertext pair, all of the keys that are obtained by differential table[4] look-up indexed on the input differences and the output differences of the 11th-round F_1 and the 12th-round F_1 as the key are wrong keys. Those keys are marked as wrong keys in a key table for distinguishing whether $RK'_{21,0} \mid RK_{22} \mid RK_{23}$ candidates[5] are correct keys or wrong keys. This method is generally used with the objective of finding the correct key by differential attacks; in impossible differential attacks, it can be used to find wrong keys without exhaustive search. The probability of a candidate for $RK'_{21,0} \mid RK_{22} \mid RK_{23}$ being a wrong key as the result of using two F_1 differential tables is 2^{-40} from the average 2^{-8} probability for the 11th-round F_1 and the average 2^{-32} probability for the 12th-round F_1. Accordingly, the number of ciphertext pairs required to narrow the candidates down to a single 72-bit correct key $RK'_{21,0} \mid RK_{22} \mid RK_{23}$, N, is about $2^{45.7}$, from

$$2^{72}(1 - 2^{-40})^N = 1.$$

From the above facts, $2^{45.7}/2^{-80} = 2^{125.7}$ plaintext pairs are required for attack. If we choose two different plaintexts from a set of 2^8 plaintexts (referred to simply as 'structure' below) for which the first three words and the first three bytes of the fourth word of the plaintext are fixed, we can make ${}_{2^8}C_2 \approx 2^{14.9}$ pairs for which the difference is $[0, 0, 0, [0, 0, 0, X]]$. In other words, it is possible to obtain the number of ciphertext pairs that are required for the attack by choosing $2^{110.8}$ $(= 2^{125.7-14.9})$ structures. In that case, the number of plaintexts is $2^{110.8} \cdot 2^8 = 2^{118.8}$.

The time complexity for attack is as follows.

1. For obtaining the ciphertexts : 2^{119} encryptions
2. For reducing the key candidates : $2^{46} \cdot 2^{32} = 2^{78}$ F-function computations $< 2^{73}$ encryptions
   (In detail, $2^{45.7}$ ciphertext pairs $\cdot$ 2^{32} RK_{22} guesses)

Accordingly, the time complexity is 2^{119} encryptions.

The memory used for attack is occupied by the key table and the ciphertext table. The size of the key table, if indexed by the key values, is 2^{72} bits. The size of the ciphertext table is 2^8 blocks (128 bits per block), if indexed by the plaintext values. Accordingly, the memory required for attack is about 2^{65} blocks.

3.3 Key Recovery Attack on 12-round CLEFIA

We extend the impossible differential attack of the 11-round CLEFIA described in Sect. 3.2 by one round on the plaintext side. In addition to RK_{22}, RK_{23}, and $RK'_{21,0}$, we can obtain the least significant byte of RK_0.

[4] A table that records the input value pairs for which occur the input-output differences for each of the input differences and output differences.

[5] To calculate the input value of the 11th-round F_1, it is necessary to try all of RK_{22}. It is therefore useful to have the $RK'_{21,0} \mid RK_{23}$ key table when guessing RK_{22}, but we chose to add RK_{22} to the key table as well to simplify the explanation of the 12-round attack in Sect. 3.3.

Movement of Whitening Key $\boldsymbol{WK_0}$. Move the whitening key WK_0, and place it at the bit-wise exclusive OR with the first round output $x^{\{1,0\}}$.

Plaintext Choice Method. Prepare a data set that comprises 2^{40} plaintexts in which the first three bytes of the first word, and the third and fourth words of the plaintext are fixed as shown in Fig. 5. In other words, there are 2^{40} plaintexts for which the first three bytes of the fourth word $x^{\{1,3\}}$, the second word $x^{\{1,1\}}$, and the third word $x^{\{1,2\}}$ are fixed, if taken as the first-round output. If, for each value of the first word $x^{\{1,0\}}$ of the first-round output, it is possible to choose 2^8 plaintexts for which the least significant bytes of the fourth word $x^{\{1,3\}}$ are different (i.e., structures), the attack described in Sect. 3.2 can be applied.

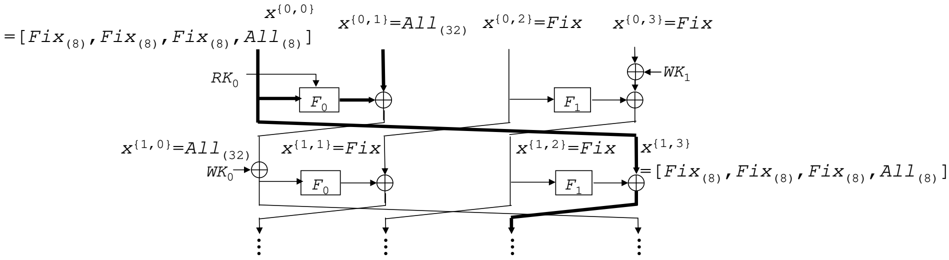

Fig. 5. Choice of plaintext for a one-round extension

Let the first word $x^{\{0,0\}}$ of the plaintext be $[a_{(8)}, b_{(8)}, c_{(8)}, d_{(8)}]$ and let RK_0 be $[k_{0(8)}, k_{1(8)}, k_{2(8)}, RK_{0,3(8)}]$. Here, a,b, and c are arbitrary fixed values, and d is a variable that takes values from 0 to 255 in order. Using this variable to express the first word $x^{\{1,0\}}$ of the first-round output, we get

$$\begin{aligned} x^{\{1,0\}} &= M_0\,{}^t[S_0(a \oplus k_0), S_1(b \oplus k_1), S_0(c \oplus k_2), 0] \\ &\oplus M_0\,{}^t[0, 0, 0, S_1(d \oplus RK_{0,3})] \oplus x^{\{0,1\}}. \end{aligned} \tag{7}$$

The first term on the right side of (7) is a fixed value.

To choose 2^8 plaintexts (structure) such that the least significant bytes of $x^{\{1,3\}}$ are all different for each value of $x^{\{1,0\}}$, we guess $RK_{0,3}$ and choose the data for which $x^{\{0,1\}}$ is $x^{\{1,0\}} \oplus M_0\,{}^t[0, 0, 0, S_1(d \oplus RK_{0,3})]$ corresponding to the change in d. Here, $x^{\{1,0\}}$ is actually the unknown value $x^{\{1,0\}} \oplus M_0\,{}^t[S_0(a \oplus k_0), S_1(b \oplus k_1), S_0(c \oplus k_2), 0]$, but when choosing a single structure, we can fix the value of $x^{\{1,0\}}$. As a result, 2^{32} structures can be chosen for the first-round output.

Key Recovery. Because an attack in the same way as described in Sect. 3.2 is possible, this description follows the procedure of that section.

From among the ciphertext pairs that correspond to the plaintext pairs for which the second-round input difference is $[0, 0, 0, [0, 0, 0, X]]$, choose those for which the ciphertext difference is $[0, [Y, 0, 0, 0], \beta, \gamma]$. The probability of obtaining such ciphertext pairs is 2^{-80}.

For the chosen ciphertext pair, the keys for which the 10th-round output difference $[\Delta x^{\{10,0\}}, \Delta x^{\{10,1\}}, \Delta x^{\{10,2\}}, \Delta x^{\{10,3\}}]$ is $[0, 0, [Y, 0, 0, 0], 0]$ are wrong keys. Prepare a key table to distinguishing whether the $RK'_{21,0} \,|\, RK_{22} \,|\, RK_{23}$ candidate is correct or wrong for each first-round guessed key $RK_{0,3}$. Keys obtained by differential table look-up with the input differences and the output differences for the 11th-round F_1 and the 12th-round F_1 are wrong keys. The probability of a wrong key obtained as an $RK'_{21,0} \,|\, RK_{22} \,|\, RK_{23}$ candidate using the two differential tables is 2^{-40}. Accordingly, the number of ciphertext pairs needed to narrow the 8-bit keys $RK_{0,3}$ and 72-bit keys $RK'_{21,0} \,|\, RK_{22} \,|\, RK_{23}$ down to the correct key, N, is $2^{45.8}$ according to

$$2^{80}(1 - 2^{-40})^N = 1.$$

When key $RK_{0,3}$ is wrong, all of the keys are wrong.

From the above description, $2^{45.8}/2^{-80} = 2^{125.8}$ plaintext pairs are required for attack. Here, by changing the order of choosing the plaintext-ciphertext pairs according to the guessing of key $RK_{0,3}$, the number of chosen plaintexts does not increase when guessing key $RK_{0,3}$. If we choose two different plaintexts from a single structure seen in the first-round output, we can make ${}_{2^8}C_2 \approx 2^{14.9}$ pairs for which the difference is $[0, 0, 0, [0, 0, 0, X]]$. That is to say, if we prepare $2^{78.9}$ $(= 2^{125.8-32-14.9})$ sets of 2^{40} plaintexts (2^{32} structures) for which the first three bytes of the first word and the third and fourth words of the plaintext are fixed, we can obtain the number of ciphertext pairs required for attack. The number of plaintexts in that case is $2^{78.9} \cdot 2^{40} = 2^{118.9}$. The difference in the required number of plaintexts with Sect. 3.2 ($2^{118.8}$) arises from the difference in the number of ciphertext pairs N required to narrow down the keys to the one correct remaining key using the key table.

The time complexity required for attack is as follows.

1. For obtaining the ciphertexts : 2^{119} encryptions
2. For reducing the key candidates : $2^8 \cdot 2^{46} \cdot 2^{32} = 2^{86}$ F-function computations $< 2^{82}$ encryptions
   (In detail, $RK_{0,3}$ guesses $2^8 \cdot$ ciphertext pairs $2^{45.8} \cdot RK_{22}$ guesses 2^{32})

Accordingly, the time complexity is 2^{119} encryptions.

The memory used for attack is occupied by the key table and the ciphertext table. The key table size is 2^{80} bits and the ciphertext table size is 2^{40} blocks. Accordingly, the memory size required for attack is about 2^{73} blocks.

3.4 Key Recovery Attacks on 13 and 14-round CLEFIA

We present a 13-round CLEFIA attack for the key length of 192 bits or more shown in Fig. 6 and a 14-round CLEFIA attack for the key length of 256 bits.

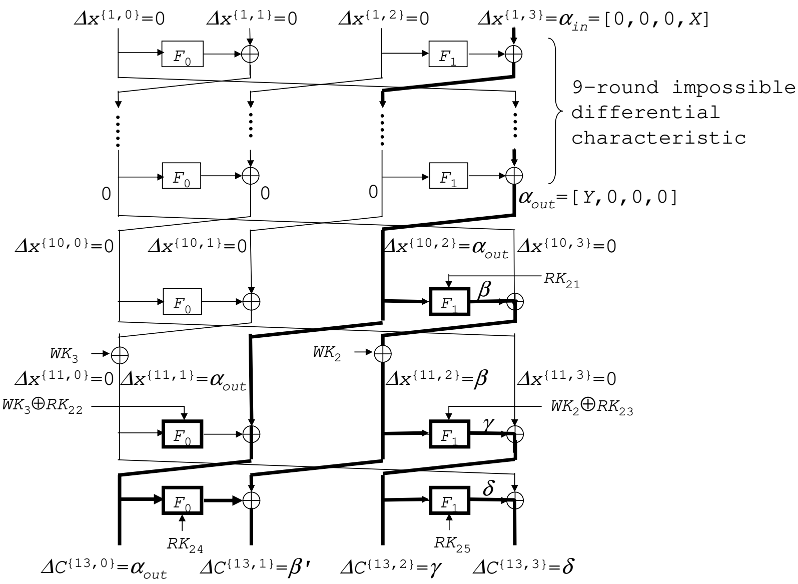

Fig. 6. Impossible differential attack on 13-round CLEFIA

In the 13-round attack, it is possible to obtain $RK_{0,3}$, the most significant byte of RK_{21} (denoted as $RK_{21,0(8)}$), $WK_3 \oplus RK_{22}$, $WK_2 \oplus RK_{23}$, RK_{24} and RK_{25}. In the 14-round attack, it is possible to obtain $RK_{0,3}$, the most significant byte of $WK_3 \oplus RK_{21}$, RK_{22}, RK_{23}, $WK_3 \oplus RK_{24}$ and $WK_2 \oplus RK_{25}$, RK_{26}, and RK_{27}. In the same way as done in Sects. 3.2 and 3.3, we first present the attack procedure for the 12 rounds from the second round to the 13th round. Then, we extend one round on the plaintext side. Finally, we explain the 14-round attack.

Movement of Whitening keys WK_0, WK_2, and WK_3. The whitening keys WK_0, WK_2, WK_3 are moved in the same way as in Sects. 3.2 and 3.3.

Key Recovery on 12-round CLEFIA. We choose the ciphertext pairs for which the first round output difference is $[0,0,0,[0,0,0,X]]$ and the 12th-round output difference is $[[Y,0,0,0],\beta,\gamma,0]$ for use in attack. Here, β represents the 255 values that can be obtained as the output difference when the input difference for M_1 is $[Y,0,0,0]$; γ is a non-zero value.

From among the ciphertext pairs that correspond to the plaintext pairs for which the first round output difference is $[0,0,0,[0,0,0,X]]$, select those for which the differences are $[[Y,0,0,0],\beta'_{(32)},\gamma,\delta_{(32)}]$. Here, β' is the bit-wise exclusive OR of the 255 values that β can take with the 255 values that the M_0 output difference can take for the case in which the input difference of M_0 is

$[Y, 0, 0, 0]$, or $255 \cdot 255 \approx 2^{16}$. The γ and δ are non-zero values. The probability of obtaining such ciphertext pairs is

$$255/2^{32} \cdot (255 \cdot 255)/2^{32} \cdot (2^{32} - 1)/2^{32} \cdot (2^{32} - 1)/2^{32} \approx 2^{-40}.$$

From among the chosen ciphertext pairs, classify the ciphertext pairs for which the 12th-round output difference is $[[Y, 0, 0, 0], \beta, \gamma, 0]$ by guessing the most significant byte of RK_{24}. Among the ciphertext pairs for which the difference is $[[Y, 0, 0, 0], \beta', \gamma, \delta]$, the probability that a usable ciphertext pair exists for each value of the most significant byte RK_{24} is 2^{-8}.

The keys for which the 10th-round output difference is $[0, 0, [Y, 0, 0, 0], 0]$ are wrong keys. Prepare a table (key table) for distinguishing $RK_{21,0} \,|\, (WK_2 \oplus RK_{23}) \,|\, RK_{25}$ candidates as correct or wrong. Then, use the input differences and output differences for the 11th-round and 12th-round F_1s and the 13th-round F_1 for look-up in the differential table and mark the obtained keys as wrong. Here, to calculate the input values of the 11th-round F_1 and the 12th-round F_1, we guess the least significant three bytes of RK_{24} and all of $WK_3 \oplus RK_{22}$. The input of the 12th-round F_0 can be calculated using the RK_{25} candidates.

The probability of knowing that a $RK_{21,0} \,|\, (WK_2 \oplus RK_{23}) \,|\, RK_{25}$ candidate is wrong by using the differential table for the three F_1s is 2^{-72}, from the average of 2^{-8} for the 11th-round F_1 and the average of 2^{-32} for the 12th-round and 13th-round F_1. Accordingly, the number of ciphertext pairs, N, required to narrow the 72-bit key $RK_{21,0} \,|\, (WK_2 \oplus RK_{23}) \,|\, RK_{25}$ and 64-bit key $RK_{24} \,|\, (WK_3 \oplus RK_{22})$ down to the correct key is about $2^{78.6}$ from

$$2^{136}(1 - 2^{-72})^N = 1.$$

From the above description, the number of plaintext pairs required for attack is $2^{78.6-40-8} = 2^{126.6}$.

If we choose two plaintexts from the same structure, we can make ${}_{2^8}C_2 \approx 2^{14.9}$ pairs for which the difference is $[0, 0, 0, [0, 0, 0, X]]$. That is to say, if we choose $2^{111.7} (= 2^{126.6-14.9})$ structures, we can obtain the number of ciphertext pairs required for attack. In that case, the number of plaintexts is $2^{111.7} \cdot 2^8 = 2^{119.7}$.

Key Recovery on 13-round CLEFIA. We extend the method for attack the 12-round CLEFIA that is described above by one round on the plaintext side to break 13-round CLEFIA.

The number of ciphertext pairs, N, required to narrow down the 8-bit key $RK_{0,3}$, the 72-bit key $RK_{21,0} \,|\, (WK_2 \oplus RK_{23}) \,|\, RK_{25}$ and the 64-bit key $RK_{24} \,|\, (WK_3 \oplus RK_{22})$ to the one correct key using the key table is $2^{78.7}$ according to

$$2^{144}(1 - 2^{-72})^N = 1.$$

The method for choosing structures for each value of the first word $x^{\{1,0\}}$ of the first round output is the same as described in Sect. 3.3, so the number of chosen plaintexts on the plaintext side is extended by N. Accordingly, the number of plaintexts required is $2^{119.8}$.

Prepare $2^{79.8}$ sets of 2^{40} plaintexts for which the first three bytes of the first word and the third and fourth words are fixed ($2^{119.8}$ plaintexts in total). Regarding these plaintexts at the first round output, we can consider them to be $2^{79.8}$ sets of 2^{40} plaintexts with the first three bytes of the fourth word and second and third words fixed. We save these $2^{119.8}$ plaintexts in a table, guess $RK_{0,3}$, and choose the plaintext pairs and use them in attack. The reason for saving all of the data, which differs from the procedure of Sect. 3.3, is that there are more keys to be guessed on the ciphertext side, and it is not possible to have a key table for them.[6]

The time complexity required for attack is as follows.

1. For obtaining the ciphertexts : $2^{119.8}$ encryptions
2. For reducing the key candidates : $2^8 \cdot 2^{78.7} \cdot 2^{64} = 2^{150.7}$ F-function computations $< 2^{146}$ encryptions
   (In detail, 2^8 $RK_{0,3}$ guesses $\cdot$ $2^{78.7}$ ciphertext pairs $\cdot$ 2^{64} $WK3 \oplus RK_{22}$ and RK_{24} guesses)

Accordingly, the time complexity is 2^{146} encryptions.

The memory used for attack is occupied by the key table and the ciphertext table. The size of the key table is 2^{72} bits; the size of the ciphertext table is $2^{119.8}$ blocks. Accordingly, the memory required for attack is about 2^{120} blocks.

Key Recovery on 14-round CLEFIA. 14-round CLEFIA can be broken by adding exhaustive search of the 14th-round keys RK_{26} and RK_{27} to the 13-round attack. The number of chosen plaintexts required for attack is $2^{120.3}$, because the number of ciphertext pairs, N, required for narrowing the keys down to the correct key using the key table is about $2^{79.2}$, from

$$2^{208}(1 - 2^{-72})^N = 1.$$

The time complexity is as follows.

1. For obtaining the ciphertexts : $2^{120.3}$ encryptions
2. For reducing the key candidates : $2^8 \cdot 2^{79.2} \cdot 2 \cdot 2^{128} = 2^{216.2}$ F-function computations $< 2^{212}$ encryptions
   (In detail, $2^8 RK_{0,3}$ guesses $\cdot 2^{79.2}$ ciphertext pairs $\cdot$ 2^{128} guesses for RK_{22}, $WK3 \oplus RK_{26}$ and RK_{27} guesses)

Accordingly, the time complexity is 2^{212} encryptions.

The memory used for attack is occupied by the key table and the ciphertext table. The size of the key table is 2^{72} bits; the size of the ciphertext table is $2^{120.3}$ blocks. Accordingly, the amount of memory required for attack is about 2^{121} blocks.

[6] In this paper, it is not possible to have a table that exceeds 2^{128} blocks.

4 Conclusion

We have presented previously unknown 9-round impossible differentials in CLEFIA, which are impossible differentials that exist in structures designed by using DSM. We used these impossible differentials to apply impossible differential attacks on CLEFIA. The result showed that an impossible differential attack that is more efficient than exhaustive search is possible for 128-bit key, 12-round CLEFIA. Furthermore, attack of 13-round CLEFIA and 14-round CLEFIA is possible for key lengths of 192 bits and 256 bits, respectively. The number of chosen plaintexts, the time complexity, and the amount of memory required for attack are listed in Table 2.

Table 2. Results of impossible differential attacks

Reference	Number of rounds	Key length	Chosen plaintexts	Time complexity (encryptions)	Amount of memory (blocks)
[6, 7]	10	128, 192, 256	$2^{101.7}$	2^{102}	2^{32}
[6, 7]	11	192, 256	$2^{103.5}$	2^{188}	2^{121}
[6, 7]	12*	256	$2^{103.8}$	2^{252}	2^{153}
This paper	12	128, 192, 256	$2^{118.9}$	2^{119}	2^{73}
This paper	13	192, 256	$2^{119.8}$	2^{146}	2^{120}
This paper	14	256	$2^{120.3}$	2^{212}	2^{121}

* Without whitening key

Even though the 9-round impossible differentials presented in this paper have the same number of rounds characteristic as the impossible differentials identified by the designers, our impossible differential attacks exceed the designers' evaluation by two more rounds that can be broken for each key length. That is true for the following reason. For the impossible differentials found by the designers, the length of the parts of the plaintext differences and ciphertext differences that are not zero is 32 bits, and the plaintext differences and ciphertext differences must be the same. For our impossible differentials, however, the length of those parts is 8 bits, and it is not necessary for the plaintext differences and the ciphertext differences to be the same, that is, they are truncated differences. If the number of bits for which the difference is non-zero is small, the number of round key bits related to the difference is also small. Because it is possible to obtain round keys that span many rounds, the number of rounds that can be broken can be increased. Also, because it is a truncated difference, the probability of obtaining ciphertext that can be used in attack is high, and we were able to increase the number of rounds that can be broken by reducing the number of chosen plaintexts that are required. Other reasons for the successful attack are the movement of the whitening key and the use of the differential table method that is often used in differential attacks. Because the number of CLEFIA rounds is 18 for a key length of 128 bits, 22 for a 192-bit key and 26 for a 256-bit key, the impossible differential attacks presented in this paper do not affect the security of CLEFIA. These attacks can, however, break more rounds of than other CLEFIA attack methods.

There is currently no method for guaranteeing resistance to an impossible differential attack and no method for designing a block cipher that is resistant to an impossible differential attack. Accordingly, much time should be allocated to evaluation of block cipher with respect to impossible differential attacks. Furthermore, methods for guaranteeing resistance to an impossible differential attack and methods for designing block ciphers that resist impossible differential attacks are important topics for future research.

Acknowledgments. The authors would like to thank Takeshi Kawabata, Hiroki Nakashima, Takahiko Syouji, and Akira Nozawa for their helpful comments.

References

1. 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.
2. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", CRYPTO'90, LNCS 537, pp. 2–21, Springer-Verlag, 1990.
3. M. Matsui, "Linear Cryptanalysis Method for DES Cipher", EUROCRYPT'93, LNCS 765, pp. 386–397, Springer-Verlag, 1994.
4. 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.
5. T. Shirai and K. Shibutani, "On Feistel Structures Using a Diffusion Switching Mechanism," FSE 2006, LNCS 4047, pp. 41–56, Springer-Verlag, 2006.
6. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit Blockcipher CLEFIA (Extended Abstract)," FSE 2007, LNCS 4593, pp. 181–195, Springer-Verlag, 2007.
7. Sony Corporation. The 128-bit Blockcipher CLEFIA, Security and Performance Evaluations, Revision 1.0, June 1, 2007. Available at http://www.sony.co.jp/Products/clefia/ .