Impossible Differential Cryptanalysis of CLEFIA*

Bing Sun[1], Ruilin Li[1], Mian Wang[2], Ping Li[1] and Chao Li[1]

[1] Department of Mathematics and System Science, Science College of National University of Defence Technology, Changsha, China, 410073
[2] Jiangnan Institute of Computing Technology, Wuxi, China, 214083
{happy_come,securitylrl}@163.com

Abstract. This paper mainly discussed the impossible differential cryptanalysis on CLEFIA which was proposed in FSE2007. New 9-round impossible differentials which are different from the previous ones are discovered. Then these differences are applied to the attack of reduced-CLEFIA. For 128-bit case, it is possible to apply an impossible differential attack to 12-round CLEFIA which requires $2^{110.93}$ chosen plaintexts and the time complexity is 2^{111}. For 192/256-bit cases, it is possible to apply impossible differential attack to 13-round CLEFIA and the chosen plaintexts and time complexity are $2^{111.72}$ and 2^{158} respectively. For 256-bit cases, it needs $2^{112.3}$ chosen plaintexts and no more than 2^{199} encryptions to attack 14-round CLEFIA and 2^{113} chosen plaintexts to attack 15-round 256-bit CLEFIA with the time complexity less than 2^{248} encryptions.
Key words: block cipher, impossible differential, CLEFIA.

1 Introduction

CLEFIA[1, 2], proposed by SONY corporation, is a newly designed 128-bit block cipher which supports 128-bit, 192-bit and 256-bit keys. The fundamental structure of CLEFIA is a generalized Feistel structure consisting of 4 data lines. There are two 32-bit F-functions per round which use two different S-boxes and two different diffusion matrices respectively. The key scheduling part shares the generalized Feistel structure with the data processing part. The number of rounds can be 18, 22 and 26 for 128-bit, 192-bit and 256-bit keys, respectively.

In [1, 3], the strength of CLEFIA against some well-known attacks were examined by the designers, including differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis, truncated differential cryptanalysis, related-key cryptanalysis and some other well-known attacks. In [4], the strength against differential fault analysis was studied, the authors showed that only about 18 faulty ciphertexts are needed to recover the entire 128-bit secret key and about 54 faulty ciphertexts for 192/256-bit keys. In [5], with some new

* The work in this paper is partially supported by the Natural Science Foundation of China (No:60573028).

tricks, the authors explored more efficient attack against the reduced version of CLEFIA which is better than the result of [3]. Also in [6], impossible differential cryptanalysis is applied to CLEFIA, new 9-round impossible differences are given which can be applied to 12-round CLEFIA with 128-bit keys and 14-round CLEFIA with 192/256-bit keys.

Impossible differences are differences that never occur. It was first applied against Skipjack[7] to reject wrong key candidates by using input difference and output difference pairs whose probabilities are zero. 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 [1, 3] 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 192/256 bits, 11-round and 12-round impossible differential attacks are possible.

However, the impossible differences given by [3] are structure-dependent and have little relations with the components CLEFIA used for example the S-boxes S_0 and S_1, the matrices M_0 and M_1. And the impossible differences given by [6] only have relations with the branch number of the matrices. In this paper, we analyzed the properties of matrices M_0 and M_1, then we show that there are previously unknown 9-round impossible differentials in CLEFIA and report our results of impossible differential attacks using those impossible differentials. The impossible differences given by [3] are included in our impossible differences and a more simple proof of the impossibility will be given in this paper.

2 Description of CLEFIA

2.1 Notations

In this paper, we will use the following notations:

F_q	finite field with q elements
$a \oplus b$	bit wise exclusive OR of a and b
$a\|b$	concatenation of a and b
Δx	difference of x
a^T	the transposition of a vector a
$a_{(n)}$	an n-bit byte
$w(a)$	the number of nonzero elements of $a \in F_{2^8}^4$
$[x_i^0, x_i^1, x_i^2, x_i^3]$	output of the i-th round, $x_i^j \in \{0,1\}^{32}$

2.2 Structures

Since the key scheduling part has little relation with our analysis, we only explain the data processing part of CLEFIA.

CLEFIA is a block cipher that has a block length of 128 bits and the key length can be 128, 192 and 256-bit respectively. The data processing part is a four-branch generalized Feistel structure with two parallel F functions—-to be exactly, F_0 and F_1, respectively—-every round. The encryption function ENC_r generates 128-bit ciphertext (C_0, C_1, C_2, C_3) from 128-bit plaintext (P_0, P_1, P_2, P_3), $2r$ 32-bit round keys $(RK_{0(32)}, RK_{1(32)}, \cdots, RK_{2r-1(32)})$, and four 32-bit whitening keys (WK_0, WK_1, WK_2, WK_3) where r is the number of round. ENC_r is defined as follows which can be depicted in Fig.1.

Step. 1. $x_0^0 = P_0, x_0^1 = P_1 \oplus WK_0, x_0^2 = P_2, x_0^3 = P_3 \oplus WK_1$,
Step. 2. For $i = 1$ to $r - 1$,
$x_i^0 = x_{i-1}^1 \oplus F_0(x_{i-1}^0, RK_{2i-2})$, $x_i^1 = x_{i-1}^2$;
$x_i^2 = x_{i-1}^3 \oplus F_1(x_{i-1}^2, RK_{2i-1})$, $x_i^3 = x_{i-1}^0$
Step. 3. $C_0 = x_{r-1}^0$, $C_1 = F_0(x_{r-1}^0, RK_{2r-2}) \oplus WK_2$
$C_2 = x_{r-1}^2$, $C_3 = F_1(x_{r-1}^2, RK_{2r-1}) \oplus WK_3$

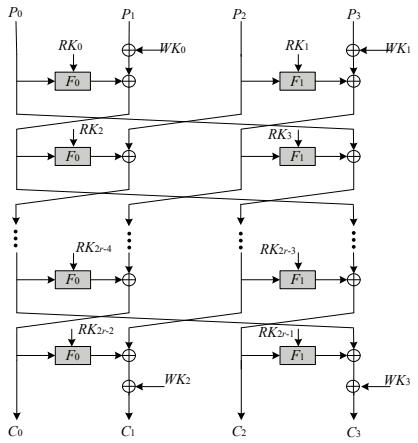

Fig. 1. Encryption Process of r-round CLEFIA(ENR_r)

F_0 and F_1 have 32-bit data x and 32-bit key RK as input and output the 32-bit data y, they are depicted in Fig.2. F_0 is defined as follows:

Step. 1. Let $x = x_{0(8)}|x_{1(8)}|x_{2(8)}|x_{3(8)}$
Step. 2. $S(x) = S_0(x_{0(8)} \oplus RK_{0(8)})|S_1(x_{1(8)} \oplus RK_{1(8)})|S_0(x_{2(8)} \oplus RK_{2(8)})|S_1(x_{3(8)} \oplus RK_{3(8)}) = z_{0(8)}|z_{1(8)}|z_{2(8)}|z_{3(8)}$
Step. 3. $y = M_0(z_{0(8)}, z_{1(8)}, z_{2(8)}, z_{3(8)})^T$

And F_1 is defined as:

Step. 1. Let $x = x_{0(8)}|x_{1(8)}|x_{2(8)}|x_{3(8)}$

Step. 2. $S(x) = S_1(x_{0(8)} \oplus RK_{0(8)}) | S_0(x_{1(8)} \oplus RK_{1(8)}) | S_1(x_{2(8)} \oplus RK_{2(8)}) | S_0(x_{3(8)} \oplus RK_{3(8)}) = z_{0(8)} | z_{1(8)} | z_{2(8)} | z_{3(8)}$

Step. 3. $y = M_1(z_{0(8)}, z_{1(8)}, z_{2(8)}, z_{3(8)})^T$

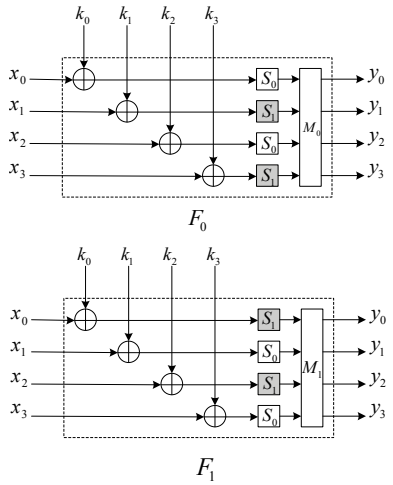

Fig. 2. The F-function F_0 and F_1

S_0 and S_1 are nonlinear 8-bit S-boxes which are bijective maps on F_{2^8}.

The two matrices used in CLEFIA are MDS matrices, and they are listed as follows(elements in the matrices are in F_{2^8} written in hex):

$$M_0 = \begin{pmatrix} 1 & 2 & 4 & 6 \\ 2 & 1 & 6 & 4 \\ 4 & 6 & 1 & 2 \\ 6 & 4 & 2 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 1 & 8 & 2 & a \\ 8 & 1 & a & 2 \\ 2 & a & 1 & 8 \\ a & 2 & 8 & 1 \end{pmatrix}$$

and the multiplications between matrices and vectors are performed in F_{2^8} defined by the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$.

3 New 9-Round Impossible Differences of CLEFIA

In [3], the author pointed that $[0, \alpha, 0, 0] \rightarrow [0, \alpha, 0, 0]$ is a 9-round impossible difference. By using this impossible differential, it is possible to attack 10-round CLEFIA with 128-bit key and 12-round CLEFIA with 192/256-bit key. In [6], new impossible differentials were given for example $[0, 0, 000\alpha, 0] \rightarrow [0, 0, 00\beta 0, 0]$ is an impossible differential. And by using the newly found characters, it is possible to attack 12-round CLEFIA with 128-bit key and 14-round CLEFIA with 192/256-bit key.

Proposition 1. *Let* $M = M_0^{-1}M_1 = (m_{ij})_{0\le i\le 3, 0\le j\le 3}$*, where* M_0 *and* M_1 *are defined as in CLEFIA. Then*

$$\begin{vmatrix} m_{i_1,j_1} & m_{i_1,j_2} \\ m_{i_2,j_1} & m_{i_2,j_2} \end{vmatrix} \neq 0$$

for $0 \le i_1 < i_2 \le 3$ *and* $0 \le j_1 < j_2 \le 3$.

Proof. It can be easily computed that

$$M = M_0^{-1}M_1 = \begin{pmatrix} 37 & 46 & 34 & 40 \\ 46 & 37 & 40 & 34 \\ 34 & 40 & 37 & 46 \\ 40 & 34 & 46 & 37 \end{pmatrix}.$$

where elements of the matrix are written in hex. Then for every $0 \le i_1 < i_2 \le 3$ and $0 \le j_1 < j_2 \le 3$, by computing the determinant

$$\begin{vmatrix} m_{i_1,j_1} & m_{i_1,j_2} \\ m_{i_2,j_1} & m_{i_2,j_2} \end{vmatrix} = m_{i_1,j_1}m_{i_2,j_2} \oplus m_{i_1,j_2}m_{i_2,j_1},$$

we can reach the required conclusion.

Theorem 1. *Differentials in the following two tables are all 9-round impossible differentials of CLEFIA where letters in bold stand for nonzero differences:*

Table.1.

α_{in}	α_{out}		
$[0, 000\mathbf{a}, 0, 0]$	$[0, 00\mathbf{d}e, 0, 0]$,	$[0, 0\mathbf{d}0e, 0, 0]$,	$[0, \mathbf{d}00e, 0, 0]$
$[0, 00\mathbf{a}0, 0, 0]$	$[0, 0\mathbf{d}e0, 0, 0]$,	$[0, \mathbf{d}0e0, 0, 0]$,	$[0, 00e\mathbf{d}, 0, 0]$
$[0, 0\mathbf{a}00, 0, 0]$	$[0, \mathbf{d}e00, 0, 0]$,	$[0, 0e0\mathbf{d}, 0, 0]$,	$[0, 0e\mathbf{d}0, 0, 0]$
$[0, \mathbf{a}000, 0, 0]$	$[0, e00\mathbf{d}, 0, 0]$,	$[0, e0\mathbf{d}0, 0, 0]$,	$[0, e\mathbf{d}00, 0, 0]$
$[0, 0, 0, 000\mathbf{a}]$	$[0, 0, 0, 00\mathbf{d}e]$,	$[0, 0, 0, 0\mathbf{d}0e]$,	$[0, 0, 0, \mathbf{d}00e]$
$[0, 0, 0, 00\mathbf{a}0]$	$[0, 0, 0, 0\mathbf{d}e0]$,	$[0, 0, 0, \mathbf{d}0e0]$,	$[0, 0, 0, 00e\mathbf{d}]$
$[0, 0, 0, 0\mathbf{a}00]$	$[0, 0, 0, \mathbf{d}e00]$,	$[0, 0, 0, 0e0\mathbf{d}]$,	$[0, 0, 0, 0e\mathbf{d}0]$
$[0, 0, 0, \mathbf{a}000]$	$[0, 0, 0, e00\mathbf{d}]$,	$[0, 0, 0, e0\mathbf{d}0]$,	$[0, 0, 0, e\mathbf{d}00]$

Table.2.

α_{in}			α_{out}
$[0, 00\mathbf{d}e, 0, 0]$,	$[0, 0\mathbf{d}0e, 0, 0]$,	$[0, \mathbf{d}00e, 0, 0]$	$[0, 000\mathbf{a}, 0, 0]$
$[0, 0\mathbf{d}e0, 0, 0]$,	$[0, \mathbf{d}0e0, 0, 0]$,	$[0, 00e\mathbf{d}, 0, 0]$	$[0, 00\mathbf{a}0, 0, 0]$
$[0, \mathbf{d}e00, 0, 0]$,	$[0, 0e0\mathbf{d}, 0, 0]$,	$[0, 0e\mathbf{d}0, 0, 0]$	$[0, 0\mathbf{a}00, 0, 0]$
$[0, e00\mathbf{d}, 0, 0]$,	$[0, e0\mathbf{d}0, 0, 0]$,	$[0, e\mathbf{d}00, 0, 0]$	$[0, \mathbf{a}000, 0, 0]$
$[0, 0, 0, 00\mathbf{d}e]$,	$[0, 0, 0, 0\mathbf{d}0e]$,	$[0, 0, 0, \mathbf{d}00e]$	$[0, 0, 0, 000\mathbf{a}]$
$[0, 0, 0, 0\mathbf{d}e0]$,	$[0, 0, 0, \mathbf{d}0e0]$,	$[0, 0, 0, 00e\mathbf{d}]$	$[0, 0, 0, 00\mathbf{a}0]$
$[0, 0, 0, \mathbf{d}e00]$,	$[0, 0, 0, 0e0\mathbf{d}]$,	$[0, 0, 0, 0e\mathbf{d}0]$	$[0, 0, 0, 0\mathbf{a}00]$
$[0, 0, 0, e00\mathbf{d}]$,	$[0, 0, 0, e0\mathbf{d}0]$,	$[0, 0, 0, e\mathbf{d}00]$	$[0, 0, 0, \mathbf{a}000]$

Proof. As an example, we give the proof that $[0, 000\mathbf{a}, 0, 0] \rightarrow [0, 0\mathbf{d}0e, 0, 0]$ where $\mathbf{a} \neq 0$ and $\mathbf{d} \neq 0$ is an impossible difference of 9-round CLEFIA. This impossible difference is depicted as Fig.3.

We can check that after the forth found, difference of x_4^3 must be of the form

$$\Delta_{x_4^3} = M_0 \begin{pmatrix} 0 \\ 0 \\ 0 \\ \mathbf{b} \end{pmatrix} \oplus M_1 \begin{pmatrix} 0 \\ 0 \\ 0 \\ \mathbf{c} \end{pmatrix}$$

Since S_0 and S_1 are bijective maps over F_{2^8}, and $b = S_1(x \oplus \mathbf{a}) \oplus S_1(x)$, $c = S_0(y \oplus \mathbf{a}) \oplus S_0(y)$ for some $\mathbf{a}, x, y \in F_{2^8}$ and $\mathbf{a} \neq 0$, thus $\mathbf{b} \neq 0$ and $\mathbf{c} \neq 0$.

By using the same trick from the backward direction, we can find that difference of x_6^1 must be of the form

$$\Delta_{x_6^1} = M_1 \begin{pmatrix} 0 \\ \mathbf{f} \\ 0 \\ g \end{pmatrix}$$

where $\mathbf{f} \neq 0$. Since $\Delta_{x_6^0}$ is of the form $(0\mathbf{d}0e)^T (\mathbf{d} \neq 0)$, after passing F_0, the difference must be $M_0(0\mathbf{h}0i)^T$ for some nonzero $\mathbf{h}$. Therefore

$$M_0 \begin{pmatrix} 0 \\ 0 \\ 0 \\ \mathbf{b} \end{pmatrix} \oplus M_1 \begin{pmatrix} 0 \\ 0 \\ 0 \\ \mathbf{c} \end{pmatrix} = M_0 \begin{pmatrix} 0 \\ \mathbf{h} \\ 0 \\ i \end{pmatrix} \oplus M_1 \begin{pmatrix} 0 \\ \mathbf{f} \\ 0 \\ g \end{pmatrix}$$

Thus

$$M_0^{-1} M_1 \begin{pmatrix} 0 \\ \mathbf{f} \\ 0 \\ \mathbf{c} \oplus g \end{pmatrix} = \begin{pmatrix} 0 \\ \mathbf{h} \\ 0 \\ \mathbf{b} \oplus i \end{pmatrix}$$

where $\mathbf{f} \neq 0$ and $\mathbf{h} \neq 0$.

By using the notations in Proposition 1, we have

$$\begin{pmatrix} m_{0,1} & m_{0,3} \\ m_{2,1} & m_{2,3} \end{pmatrix} \begin{pmatrix} \mathbf{f} \\ \mathbf{c} \oplus g \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Since $\begin{vmatrix} m_{0,1} & m_{0,3} \\ m_{2,1} & m_{2,3} \end{vmatrix} \neq 0$, the equation above has only zero solution. Thus $\mathbf{f} = 0$, $\mathbf{c} \oplus g = 0$ which is contradict with $\mathbf{f} \neq 0$.

Note. It is obviously that if $e = 0$, they are exactly the ones given by [6].

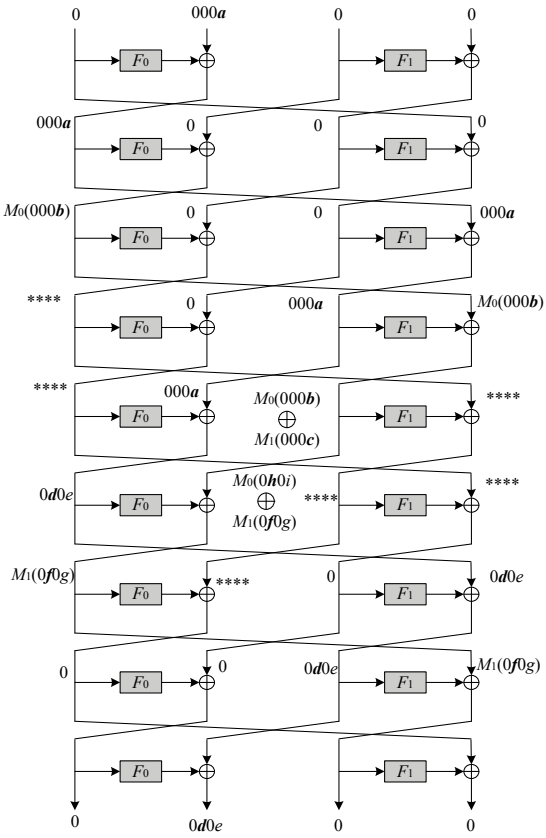

Fig. 3. 9-Round Impossible Difference of CLEFIA

4 Attacks on CLEFIA

In this section, we describe impossible differential attacks on reduced-round CLEFIA by using our new 9-round impossible differentials. To decrease the time complexity, our attack will take advantage of [5]. We first list an useful proposition stated in [5].

Proposition 2. *For the F-function(F_0 or F_1), let (In, In') be two 32-bit inputs, and Δ_{out} be the difference of the corresponding output, the 32-bit round subkey RK involved in F can be deduced with about one F-computation.*

The proof of proposition 2 is appeared in [5]. This proposition states that, if the input pair and the corresponding differentials of F-functions are known, then we can compute the keys used in F-function by only one calculation. To apply our attack efficiently, we need the following proposition.

Proposition 3. *Let $\omega_i = \{r | r = (r_0, r_1, r_2, r_3)^T, r_t = 0 \text{ if } t \neq i\}$, $\omega_{ij} = \{r | r = (r_0, r_1, r_2, r_3)^T, r_t = 0 \text{ if } t \neq i \text{ or } j\}$. $\Lambda_i = \{v | v = M_0 r_1 \oplus M_1 r_2, r_1, r_2 \in \omega_i\}$, $\Lambda_{ij} = \{v | v = M_0 r_1 \oplus M_1 r_2, r_1, r_2 \in \omega_{ij}\}$, then for any $\gamma \in \Lambda_i(\Lambda_{ij})$, there exists unique $v_1, v_2 \in \omega_i(\omega_{ij})$, such that $\gamma = M_0 v_1 \oplus M_1 v_2$.*

The proof is similar to Theorem 1. Details are omitted.

In description of the attack, a $*$ always stands for an unknown byte-difference which is not equal to 0.

4.1 Key Recovery Attack on 12-round CLEFIA

The 12-round impossible differential attack of CLEFIA uses the 9-round impossible differentials with additional one round at the beginning and two rounds at the end as in Fig. 4 .

Let $\phi = (x_0, x_1, x_2, x_3)$ where $x_i \in \{0,1\}^{32} (i = 0, 1, 2, 3)$ are constant and $\Lambda = (0, 0, 00**, M_1(00**))$. Then a structure X_ϕ is defined as $X_\phi = \{\phi \oplus \lambda | \lambda \in \Lambda\}$, thus there are $(2^8 - 1)^4 \approx 2^{32}$ elements in X_ϕ.

1. Take $2^{78.93}$ structures ($2^{110.93}$ plaintexts, $2^{141.93}$ pairs). Choose pairs whose ciphertext pairs have the following form $C \oplus C^* = (M_0(00*0), ****, 0, 00*0)$. The expected number of such ciphertext pair (C, C^*) is $N = 2^{141.93} \times 2^{-80} = 2^{61.93}$.
2. For the chosen pair (C, C^*) and its corresponding plaintext pair (P, P^*), guess RK_{23}(4 bytes) and then compute $RK_{22}|(WK_3 \oplus RK_{20})_2|(RK_1)_{2,3}$(7 bytes) according to Proposition 2. After analyzing the $2^{61.93}$ pairs, only about $2^{88}(1 - 2^{-56})^N \approx 1$ key will be left, and this is the right key.

The time complexity is as follows:

1. For obtaining the ciphertexts: $2^{110.93}$ encryptions
2. For reducing the key candidates: $\leq 2^{32} N = 2^{93.93}$ F-function computations.

Accordingly, the time complexity for this attack is 2^{111} encryptions.

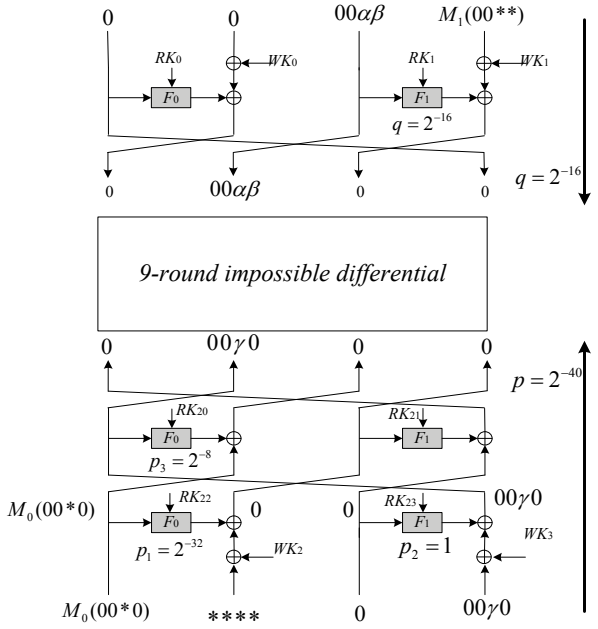

Fig. 4. 12-Round Impossible Difference attack on CLEFIA

4.2 Key Recovery Attack on 13-round CLEFIA

By adding one more round in the forward direction to the previous 12-round character, we get a 13-round impossible differential attack on CLEFIA.

Let $\phi = (x_0, x_1, x_2, x_3)$ where $x_i \in \{0,1\}^{32} (i = 0, 1, 2, 3)$ are constant and $\Lambda = (M_1(00**), ****, 0, 00**)$. Then a structure X_ϕ is defined as $X_\phi = \{\phi \oplus \lambda | \lambda \in \Lambda\}$, thus there are $(2^8 - 1)^8 \approx 2^{64}$ elements in X_ϕ.

1. Take $2^{47.72}$ structures ($2^{111.72}$ plaintexts, $2^{174.72}$ pairs). Choose pairs whose ciphertext pairs have the following form $C \oplus C^* = (M_0(00*0), ****, 0, 00*0)$. The expected number of such ciphertext pair (C, C^*) is $N = 2^{174.72} \times 2^{-80} = 2^{94.72}$.
2. For the chosen pair (C, C^*) and its corresponding plaintext pair (P, P^*), guess $RK_{25}|RK_1$(8 bytes) and compute $RK_0|(RK_3 \oplus WK_1)_{2,3}|RK_{24}|(WK_3 \oplus RK_{22})_3$(11 bytes) according to Proposition 2. After analyzing the $2^{94.72}$ pairs, only about $2^{152}(1 - 2^{-88})^N \approx 1$ key will be left, which is the right key.

The time complexity is as follows:

1. For obtaining the ciphertexts: $2^{111.72}$ encryptions
2. For reducing the key candidates: $\leq 2^{64} N = 2^{158.72}$ F-function computations.

Accordingly, the time complexity for this attack is $\leq 2^{158}$ encryptions.

4.3 Key Recovery Attack on 14-round CLEFIA

To get a 14-round impossible differential attack on CLEFIA, we add 2 rounds in the forward direction and 3 rounds in the backward direction to the previous 9-round character.

Let $\phi = (x_0, x_1, x_2, x_3)$ where $x_i \in \{0,1\}^{32} (i = 0, 1, 2, 3)$ are constant and $\Lambda = (M_1(00**), **\,**, 0, 00**)$. Then a structure X_ϕ is defined as $X_\phi = \{\phi \oplus \lambda | \lambda \in \Lambda\}$, thus there are $(2^8 - 1)^8 \approx 2^{64}$ elements in X_ϕ.

1. Take $2^{48.23}$ structures ($2^{112.23}$ plaintexts, $2^{175.23}$ pairs). Choose pairs whose ciphertext pairs have the following form $C \oplus C^* = (****, ****, 00*0, M_0(00* 0) \oplus M_1(00*0))$. The expected number of such ciphertext pair (C, C^*) is $N = 2^{175.23} \times 2^{-40} = 2^{135.23}$.
2. For the chosen pair (C, C^*) and its corresponding plaintext pair (P, P^*), we guess $RK_1|(RK_{24} \oplus WK_3)$(8 bytes), and then compute $RK_{26}|RK_{27}|(RK_{25} \oplus WK_2)|(RK_{22})_2|RK_0|(RK_3 \oplus WK_1)_{2,3}$(19 bytes) according to Proposition 2. After analyzing the $2^{135.23}$ pairs, only about $2^{216}(1 - 2^{-128})^N \approx 1$ key will be left, and this is the right key.

The time complexity is as follows:

1. For obtaining the ciphertexts: $2^{112.23}$ encryptions
2. For reducing the key candidates: $\leq 2^{64} N = 2^{199.23}$ F-function computations.

Accordingly, the time complexity for this attack is $\leq 2^{199}$ encryptions.

4.4 Key Recovery Attack on 15-round CLEFIA

By adding 3 more rounds in the forward direction and 3 rounds in the backward direction to the previous 9-round impossible differentials, we can even get a 15-round attack on 256-bit CLEFIA.

Let $\phi = (x_0, x_1, x_2, x_3)$ where $x_i \in \{0,1\}^{32} (i = 0, 1, 2, 3)$ are constant and $\Lambda = (00**, M_0(00**) \oplus M_1(00**), ****, ****)$. Then a structure X_ϕ is defined as $X_\phi = \{\phi \oplus \lambda | \lambda \in \Lambda\}$, thus there are $(2^8 - 1)^{14} \approx 2^{112}$ elements in X_ϕ.

1. Take 2 structures (2^{113} plaintexts, 2^{224} pairs). Choose pairs whose ciphertext pairs have the following form $C \oplus C^* = (** **, ** **, 00 * 0, M_0(00 * 0) \oplus M_1(00 * 0))$. The expected number of such ciphertext pair (C, C^*) is $N = 2^{224} \times 2^{-40} = 2^{184}$.
2. For the chosen pair (C, C^*) and its corresponding plaintext pair (P, P^*), we guess $RK_3 \oplus WK_1|(RK_{27} \oplus WK_2)$(8 bytes), then compute $RK_{28}|RK_{29}|(RK_{26} \oplus WK_3)|(RK_{24})_2|RK_0|RK_1|RK_2 \oplus WK_0|(RK_5)_{2,3}$(27 bytes) according to Proposition 2. After analyzing the 2^{184} pairs, only about $2^{280}(1 - 2^{-176})^N \approx 1$ key will be left, and this is the right key.

Note. We have obviously that $M_0(00**) \oplus M_1(00**) = \{0,1\}^{32}$, according to Proposition 3, the decomposition is unique which is very important in the computation of time complexity.

The time complexity is as follows:

1. For obtaining the ciphertexts: 2^{113} encryptions
2. For reducing the key candidates: $\leq 2^{64}N = 2^{248}$ F-function computations.

Accordingly, the time complexity for this attack is $\leq 2^{248}$ encryptions.

5 Conclusion

New 9-round impossible differences of CLEFIA are given in this paper. And we use the impossible differences to attack CLEFIA of reduced round. The result shows that, for 128-bit case, it is possible to apply an impossible differential attack to 12-round CLEFIA which requires $2^{110.93}$ chosen plaintexts and the time complexity is 2^{111}; for 192-bit case, it is possible to apply impossible differential attack to 13-round CLEFIA and the chosen plaintexts and time complexity are $2^{111.72}$ and 2^{158} respectively; for 256-bit cases, it needs $2^{112.3}$ plaintexts and no more than 2^{199} encryptions to attack 14-round CLEFIA. Besides, we can even get an attack to 15-round reduced-CLEFIA with 2^{113} chosen plaintexts and the time is no more than $\leq 2^{248}$ encryptions. These results are the best attacks on CLEFIA. These results are listed in Table.3.

Table.3. Results of Impossible Differential Attacks on CLEFIA

Reference	Number of Rounds	Key Length	Chosen Plaintexts	Time Complexity (Encryption)
[1, 3]	10	128,192,256	$2^{101.7}$	2^{102}
[1, 3]	11	192,256	$2^{103.5}$	2^{188}
[5]	11	128,192,256	$2^{103.1}$	$2^{98.1}$
[1, 3]	12*	256	$2^{103.8}$	2^{252}
[5]	12	128,192,256	$2^{119.3}$	$2^{114.3}$
[6]	12	128,192,256	$2^{118.9}$	2^{119}
this paper	12	128,192,256	$2^{110.93}$	2^{111}
[5]	13	192,256	2^{120}	2^{181}
[6]	13	192,256	$2^{119.8}$	2^{147}
this paper	13	192,256	$2^{111.72}$	$\leq 2^{158}$
[5]	14	256	$2^{120.4}$	$2^{245.4}$
[6]	14	256	$2^{120.3}$	2^{211}
this paper	14	256	$2^{112.3}$	$\leq 2^{199}$
this paper	15	256	2^{113}	$\leq 2^{248}$

From the table we can find that, comparing with [6], the number of chosen plaintexts is much decreased, this is because that, the Hamming weight of the

input to impossible differentials are $w(a) = 1$ in [6] and $w(a) = 1$ in ours, which means that, in the backward direction, our attack is almost the same with [6] while in the forward direction, plaintexts in a structure is much larger than that of [6]. In other words, to get the same number of pairs, the differentials in this paper is better than that of [6].

To avoid this kind of new impossible differentials, instead of using M_0 and M_1 in F_0 and F_1 respectively, we can use only, for example, M_0 in both F_0 and F_1. Then the proof will be invalid for this case.

References

1. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit Blockcipher CLEFIA. In: Biryukov, A. (ed.) FSE 2007, vol. 4593, pp. 181-195. Springer, Heidelberg (2007)
2. Sony Corporation. The 128-bit Blockcipher CLEFIA: Algorithm Specification. Revision 1.0 June 1, 2007.
3. Sony Corporation. The 128-bit Blockcipher CLEFIA: Security and Performance Evaluation. Revision 1.0 June 1, 2007.
4. H. Chen, W. Wu, and D. Feng, Differential Fault Analysis on CLEFIA. ICICS 2007(S. Qing, H. Imai, and G. Wang, Eds), pp. 284-295, Springer-Verlag, 2007.
5. W. Wang and X.Y. Wang, Improved Impossible Differential Cryptanalysis of CLEFIA. http://eprint.iacr.org2007/466.pdf
6. Y. Tsunoo, E. Tsujihara2, M. Shigeri, T. Saito, T. Suzaki, and H. Kubo, Impossible Differential Cryptanalysis of CLEFIA. to be appeared in FSE2008.
7. E. Biham, A. Biryukov, and A. Shamir, Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials, EUROCRYPT99, LNCS 1592, pp. 12-23, Springer-Verlag, 1999.